SEGURANÇA COM IPv6 - UM ESTUDO SOBRE AS VULNERABILIDADES

João Eduardo Araújo de Meneses[1]

Humberto Caetano Cardoso da Silva[2]

Resumo

A migração para o novo Protocolo da Internet (IPv6), faz-se cada vez mais urgente devido à extinção de endereços IPv4 e à demanda de mais segurança. Entretanto, as novas funcionalidades adicionadas no novo protocolo possibilitaram o surgimento de novas vulnerabilidades, requerendo mais atenção por parte dos administradores das redes que o adotem. Adicionalmente, várias das antigas vulnerabilidades continuam presentes na nova versão do protocolo. Este artigo tem como objetivo estudar como algumas dessas vulnerabilidades são exploradas e as técnicas de identificação e mitigação/eliminação das ameaças, apontando ferramentas para fazê-lo e contribuindo para que os gerentes consigam um grau a mais de segurança para suas redes.

Palavras-chave: IPv6, segurança da informação, vulnerabilidades, ameaças.

Abstract

Migration to the new Internet Protocol (IPv6) is becoming more urgent due to the extinction of IPv4 addresses and the demand for more security. However, the new features added in the new protocol have allowed the appearance of new vulnerabilities, requiring more attention by the administrators of the networks that adopt it. In addition, several of the old vulnerabilities are still present in the new version of the protocol. This article aims to study how some of these vulnerabilities are exploited and techniques for identifying and mitigating / eliminating threats, pointing out tools to do so and helping managers to achieve an even greater degree of security for their networks.

Keywords: IPv6, information security, vulnerabilities, threats.

[1] Especialista em Segurança de Redes Computacionais pela Faculdade Santo Agostinho.
[2] Professor da Uninassau Recife, Doutorando em Administração pela Universidade Federal de Pernambuco, Mestre em Gestão Empresarial pela Devry/FBV (MPGE/FBV).

1 INTRODUÇÃO

A internet que conhecemos hoje nasceu nos Estados Unidos na década de 60, no período da Guerra Fria. O governo americano, temendo um ataque, buscava uma forma de descentralizar e trocar informações de forma sigilosa. Assim, criou-se a rede ARPANET. Depois, o governo americano permitiu o uso da ARPANET pelas universidades para que fossem realizados estudos.

Devido ao grande número de universidades e suas localidades distintas, a dificuldade de administração do sistema não demorou a aparecer, tornando clara a necessidade de um novo sistema de comunicação. Então, o IP (*Internet Protocol* – Protocolo da Internet) foi concebido para transferência de dados de uma rede para outra. Assim, Todas as redes, em localidades diferentes, comunicavam-se pelo endereço IP da internet (COAN, 2013).

A partir dos anos 90 a internet começava a ser usada comercialmente, a quantidade de usuários conectados crescia exponencialmente, pois foram oferecidos vários serviços, como transação bancária e comércio eletrônico (CAMACHO, 2012). Nesse cenário, os endereços IPv4 disponíveis ficavam cada vez mais escassos e a segurança nas transações tornava-se uma necessidade. Nesse momento, o Protocolo IP vigente (IPv4) mostrava-se com problemas que não tinham sido previstos quando da sua criação (COAN, 2013):

- Crescimento das redes e esgotamento de endereços IP;
- Aumento da tabela de roteamento;
- Problemas de tráfego seguro e
- Prioridade de entrega de pacotes por tipos de tráfego.

A ideia de um novo Protocolo da Internet (IPv6) substituir o atual (IPv4) amadurecia. Hoje o IPv6 é uma realidade. Apesar de não estar completamente introduzido na Internet, o IPv6 funciona concomitantemente com o IPv4: várias organizações já migraram suas redes para IPv6 (TUVO, 2011). No projeto IPv6, destacam-se o maior espaço de endereçamento, o suporte a extensões de segurança, a simplificação do cabeçalho para um melhor desempenho da rede, a autoconfiguração, além de suportar outras extensões (GARCIA; RHODEN; WESTPHALL, 2015).

Contudo, a adição de novas funcionalidades trouxe novas vulnerabilidades, algumas descobertas e outras por descobrir, além das já existentes devido à arquitetura da Internet (*IP*

Spoofing, *Denial of Service*, etc). Assim, é fundamental que os administradores de redes possuam domínio sobre os conceitos da nova versão. (RIBEIRO, 2015).

No sentido de auxiliar esses profissionais, este estudo busca realizar um estudo sobre as novas funcionalidades do Protocolo da Internet – versão 6, sobre algumas das suas vulnerabilidades de mais fácil exploração e de maior dano para o alvo, sobre alternativas para poder mitigar seus riscos de exploração e sobre novos possíveis problemas que possam surgir. Inicialmente, são apresentados os conceitos básicos e principais funcionalidades do IPv6. Em seguida, são destacadas as principais ameaças e vulnerabilidades relativas ao IPv6. Depois, são descritas formas de detecção dos ataques e possíveis formas de defesa. E por fim, são apresentadas as considerações finais sobre o trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

Como a motivação principal para o Protocolo da Internet versão 6 foi o espaço de endereçamento, esse foi aumentado consideravelmente. Passou-se da representação de 32 bits (IPv4) para 128 bits, dividindo o endereço em oito grupos de 16 bits separados por ":" e representados por dígitos hexadecimais (0-F). Por exemplo: 2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1. Os zeros a esquerda de cada bloco de 16 bits podem ser omitidos. Também, a seqüência longa de zeros pode ser substituída por "::". Assim, o endereço 2001:0DB8:0000:0000:130F:0000:0000:140B pode ser escrito como 2001:DB8:0:0:130F::140B ou 2001:DB8::130F:0:0:140B. Para a representação de máscara de rede, a notação CIDR continua a ser utilizada no IPv6 (IPV6.BR, 2016). A notação CIDR (*Classless Inter-Domain Routing*) indica o número de bits disponíveis para representação dos endereços de rede e, por consequência, dos hosts. No exemplo 2001:db8:3003:2::10/64, os primeiros 64 bits representam a rede e os 64 bis restantes representam o host.

2.1 Endereçamento IPv6

No IPv6 existem três tipos de endereços definidos: *unicast*, *multicast* e *anycast*. Um endereço ***unicast*** identifica uma única interface. Um pacote endereçado a um endereço *unicast* será entregue unicamente à interface que o possua.

- **Global *Unicast* -** equivalente aos IPs públicos do IPv4. Estando na rede IPv6, é globalmente atingível e roteável. Está dividido em três partes: prefixo de roteamento global, identificação da sub-rede e identificação da interface (IPV6.BR, 2016).

- **Link Local** - Endereço usado apenas dentro do enlace local. Possui os 64 bits da esquerda fixos: sempre com a configuração FE80::/64. Assim, os roteadores entendem que, quando um pacote vier com um endereço de origem nessa configuração, esse não deve ser encaminhado para o exterior o enlace (RIBEIRO, 2015).

- **Unique Local** - Endereço com garantia quase total de ser globalmente único, mas que é usado apenas no enlace local (RIBEIRO, 2015).

- **Endereço de *Loop Back*** – Também conhecido como *localhost*, é o endereço que representa a própria máquina e é representado por 0:0:0:0:0:0:0:1 ou ::1. Este endereço não é encaminhado por roteadores nem deve ser usado como endereço de origem de pacotes (IPV6.BR, 2016).

- **Endereço Não-Especificado** - Representado por 0:0:0:0:0:0:0:0 ou ::0 , este endereço é usado quando do envio de pacotes que visam a autoconfiguração de endereço quando ainda não se sabe o próprio endereço. Não deve ser atribuído a nenhum nó (IPV6.BR, 2016).

Endereços ***multicast*** representam um grupo de interfaces. Um pacote com um endereço *multicast* como destino deve ser entregue a todas as interfaces que pertecem ao grupo correspondente ao endereço. Uma interface pode estar em vários grupos *multicast*. Um endereço *multicast* não pode ser usado como endereço de origem de um pacote e sempre deriva do bloco FF00::/8. Toda vez que é atribuído um endereço IPv6 *unicast* ou *anycast* na interface é atribuído também um endereço *multicast* correspondente, o *multicast solicited-node* (IPV6.BR, 2016).

Um endereço ***anycast*** também representa um grupo de interfaces. Mas, diferentemente do pacote *multicast*, que é enviado para todas as interfaces do grupo, um pacote *anycast* é enviado, somente, à interface mais próxima. Esse tipo de endereço foi criado para garantir redundância de dispositivos que disponibilizam serviços de rede como roteamento, DNS e *proxy* (RIBEIRO, 2015).

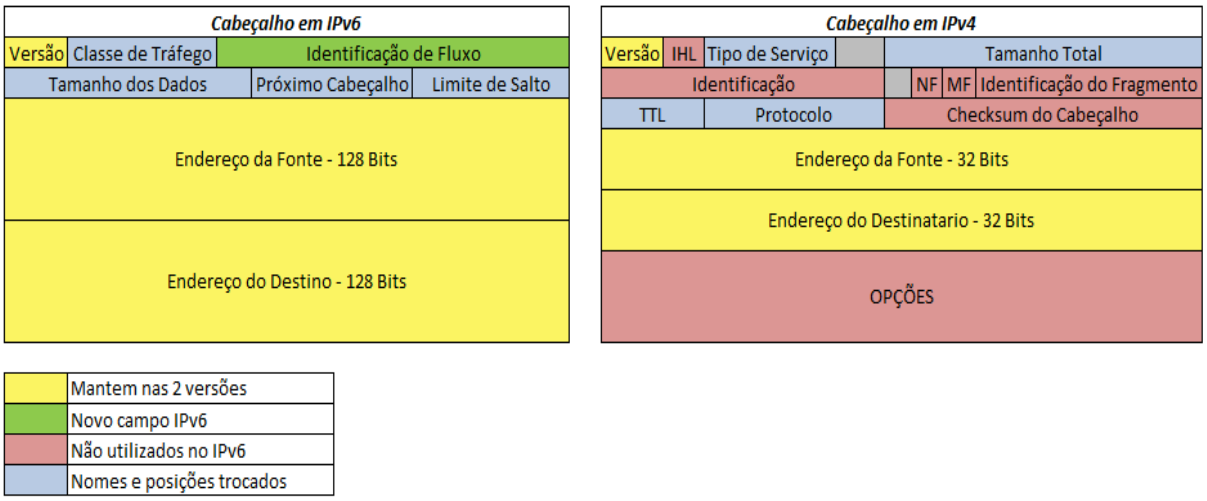
2.2 Cabeçalho IPv6

O cabeçalho IPv6 foi modificado a partir do cabeçalho IPv4 para otimizar as questões de processamento de pacotes e de segurança, eliminando campos (**Tamanho do Cabeçalho**, **Identificação**, ***Checksum* do Cabeçalho**, ***Flags***, **Identificação do Fragmento**) que eram

raramente usados e adicionando outros (**Identificação de Fluxo**) para melhor provimento de tráfego prioritário. O cabeçalho IPv6 possui o tamanho fixo de 40 *bytes*, com 32 *bytes* para os endereços de origem e destino, sobrando apenas 8 *bytes* para informações complementares (SANTOS, 2004).

No cabeçalho IPv6, O campo **Classe de Tráfego** identifica a classe ou prioridade do pacote. O campo **Identificação de Fluxo** indica a que sequência específica de pacotes trocados entre uma origem e destino, demandando o tratamento correspondente pelos roteadores intermediários. O campo **Próximo Cabeçalho** informa qual o protocolo do próximo pacote ou se é um cabeçalho de extensão. O cabeçalho IPv6 e IPv4 podem ser vistos na Figura 1 (SANTOS, 2004).

Figura 1: Diferença entre os cabeçalhos IPv4 e IPv6.



Fonte: (COAN, 2013)

Os cabeçalhos de extensão foram criados para que o cabeçalho IPv6 ficasse eficiente e flexível como era requerido em seu projeto. Esses cabeçalhos contêm informações adicionais opcionais sobre os dados do pacote e ficam entre o cabeçalho IPv6 e o da camada superior (COAN, 2013).

2.3 ICMPv6 - *Internet Control Messages Protocol* (versão 6)

Para ser utilizado com o IPv6, o protocolo ICMPv4 foi atualizado e melhorado para a versão 6. Além de realizar as funções da versão 4, como informar características da rede e sobre erros nos processamentos do pacotes, o ICMPv6 incorporou novas funcionalidades, inclusive as de outros protocolos que ficavam isolados na versão anterior, tornando-se mais

poderoso e indispensável na arquiterura IPv6. As funcionalidades agregadas foram as dos protocolos ARP (tradução de endereços físicos em endereços IPv4), RARP (tradução de endereços IPv4 em endereços físicos) e IGMP (gerenciar membros de endereços *multicast*) (RIBEIRO, 2015).

O pacote ICMPv6 é encapsulado num pacote IPv6 e tem o valor 58 no campo *Next Header* do cabeçacho IPv6 (IPV6.BR, 2016).

2.4 NDP (*Neighbor Discovery Protocol*)

Para facilitar a interação de nós vizinhos na rede, o NDP foi adicionado ao IPv6.

O NDP trouxe a possibilidade de autoconfiguração dos nós da rede. Para isso são usadas as seguintes funcionalidades do NDP (SIQUEIRA, 2011):

- ***Parameter Discovery*** - O nó utiliza essa técnica para descobrir parâmetros físicos do enlace como MTU e limite de saltos.

- ***Address Autoconfiguration*** - Funcionalidade para atribuição automática de endereços (*stateless*) da interface.

- ***Duplicate Address Detection*** - Mecanismo utilizado para detectar se o endereço que lhe foi atribuído está duplicado na rede.

Além da autoconfiguração de nós, o NDP tem funcionalidades que auxiliam na troca de pacotes entre os nós da rede (SIQUEIRA, 2011):

- ***Router Discovery*** - Técnica usada para descoberta de roteadores no mesmo segmento de rede.

- ***Prefix Discovery*** - Funcionalidade utilizada pra descoberta do prefixo da rede, que será usado para indetificar se o pacote será enviado para fora do enlace ou para um nó do próprio enlace.

- ***Address Resolution*** - Mecanismo para obtenção do endereço físico a partir do endereço IPv6 (função do protocolo ARP no IPv4).

- ***Neighbor Unreachability Detection*** - Técnica que ajuda a determinar se um vizinho está ou continua acessível.

- ***Redirect*** **-** Funcionalidade executada pelo roteador que avisa ao nó uma rota melhor para o próximo salto**.**

- ***Next-Hop Determination*** **-** Mecanismo que utiliza um algoritmo para mapear o endereço de destino nos endereços dos vizinhos a fim de determinar o próximo salto.

Para realizar todas essas funcionalidades, o protocolo NDP utiliza mensagens ICMPv6. Para isso, foram reservadas 5 delas (IPV6.BR,2015). A seguir (XAVIER; JUNIOR; MASIN; SILVA, 2012):

- ***Router Solicitation*** - esta mensagem pede que os roteadores do enlace local se apresentem mandando uma resposta *Router Advertisement*. Como destino da mensagem tem-se o endereço multicast *All-router multicast Group* (FF02::2), pois nenhum parâmetro da rede é sabido no início da conexão, e como origem da mensagem, o endereço *unicast* não-especificado (::0).

- ***Router Advertisement*** - esta mensagem é difundida, regularmente, no enlace local pelo roteador em espaços de tempo ou enviada diretamente para a interface que a solicitou via *Router Solicitation*. No caso de difusão pelo enlace, como destino tem-se o endereço multicast *All-nodes multicast Group* (FF02::1).

- ***Neighbor Solicitation*** - esta mensagem é enviada em três situações e tem como resposta uma *Neighbor Advertisiment*. Na primeira, é utilizada para descoberta de endereço físico a partir do lógico. Na segunda situação, é enviada para testes de acessibilidades dos nós. E, finalmente, na terceira, utiliza-se para detectar endereços duplicados no enlace local.

- ***Neighbor Advertisement*** - esta mensagem é enviada para todos os nós do enlace, no caso de alguma mudança nos parâmentros do dispositivo, ou para uma interface específica em resposta a uma mensagem *Neighbor Solicitation*.

- ***Redirect*** - esta mensagem é enviaada para informar aos nós do enlace uma melhor rota para o encaminhamento dos pacotes.

2.5 Segurança no IPv6

O protocolo IPv6 aprimorou sua segurança em relação ao IPv4, mas também é afetado por algumas ameaças das redes IPv4, pois são inerentes à arquitetura da Internet, como ataques à camada de aplicação, *sniffers*, negação de serviço (*Denial-of-Service - DoS*) e *man-*

in-the-middle, ainda que sejam executados de forma diferentes. Ademais, a coexistência dos protocolos IPv4 e IPv6 adicionam na rede vulnerabilidades que advém dos mecanismos de transição entre esses protocolos. Também, inicialmente, foi definido que a implementação do IPSec (protocolo de segurança do IPv6) seria obrigatória, mas, posteriormente, deixou de sê-lo (GARCIA; RHODEN; WESTPHALL, 2015).

2.5.1 IPSec - *Internet Protocol Security*

O protocolo IPSec foi criado, originalmente para o IPv4, para fornecer serviços como autenticidade, integridade e privacidade dos pacotes. Uma VPN (*Virtual Private Network*) pode usar esses serviços para prover a transmissão segura dos dados. No IPv6, o IPSec deve ser habilitado e configurado em cada nó que se deseja usá-lo e, para prover seus serviços de segurança, faz uso dos cabeçalhos de extensão do IPv6, como o AH - *Autentication Header* e ESP - *Encapsulating Security Protocol* (BEIRA, 2014).

O cabeçalho AH é usado para fornecer autenticação e integridade dos pacotes. O ESP é responsável por garantir confidencialidade através de criptografia aos dados. O IPv6 também usa o IKE - *Internet Key Exchange* para geração e gerenciamento de chaves de segurança usadas na associação (BEIRA, 2014).

O IPSec pode ser operado de dois modos: Modo Transporte e Modo Túnel. No Modo Transporte, a comunicação se dá entre dois hosts, assim o cabeçalho IP original é mantido e a autenticação e a criptografia são realizadas no *payload*. No Modo Túnel, o pacote IP original é encapsulado dentro de outro pacote IP e a comunicação é realizada entre dois roteadores, dessa forma os hosts não precisam ter o IPSec configurado como é requerido no Modo Transporte. (BEIRA, 2014).

2.5.2 SEND - Secure Neighbor Discovery

O SEND é o protocolo concebido para combater problemas inerentes do NDP, implementando comunicação segura entre os nós, conferindo-o um grau de segurança a mais. Os nós configurados com SEND utilizam criptografia de chave pública para proporcionar lisura às suas comunicações, mas têm suas cargas computacionais aumentadas. A criptografia de chave pública é utilizada na geração de novos IPs, pois, com o SEND não é permitida a autoconfiguração de IPs. O IP, nesse caso, é composto por um número aleatório, pela chave pública e pelo prefixo da subrede. A criptografia de chave pública garante autencidade no

método de atribuição do novo IP por meio de assinatura. Esse mecanismo é chamado de *Cryptographically Generated Address* (CGA) (RIBEIRO, 2015).

3 VULNERABILIDADES NO IPv6

Com todos esses novos protocolos, mecanismos e ferramentas do IPv6, surgiram novas formas de atacar a rede. Novos modos de *spoofing*, *sniffering*, *flooding*, DoS, entre outros, que buscam degradar ou paralisar serviços essenciais aos usuários. Assim, esta etapa deste artigo busca enumerar algumas vulnerabilidades de mais fácil exploração causadoras de grandes danos aos serviços de rede e como se dá essa exploração.

As ferramentas citadas adiante para exploração de vulnerabilidades estão presentes no *framework* Kali e/ou no THC-IPV6 - kit de ferramentas de ataque em redes IPv6 do *The Hacker Choice*. O *The Hacker Choice* é um grupo de pesquisadores com foco em segurança que realiza estudos em busca de falhas em protocolos e mecanismos para certificá-las a fim de que se encontrem soluções. O THC-IPV6 está presente *framework* Kali (TEIXEIRA, 2014).

3.1 Reconhecimento da Rede

Como primeiro passo de um ataque, o reconhecimento da rede faz-se conveniente para saber que tipo de rede está sendo invadida, além de quais e de que tipos são os equipamentos ligados a ela. A grande maioria dos administradores de redes releva bastante *scans* de rede, mas, se utilizados de forma elevada, podem causar aumento do consumo de largura de banda e degradação dos serviços da rede. Servidores DNS são grandes alvos de *scans* em redes IPv6, pois trabalhar com endereços IPv6 ficou muito mais difícil que com IPv4. Para realizar os *scans* em redes IPv6 podem ser usadas as mesmas ferramentas para *scans* em redes IPv4 como *nmap, ping, whois, nslookup, traceroute*, entre outras (RIBEIRO, 2015).

O procedimento de reconhecimento tornou-se mais trabalhoso em redes IPv6 devido à grande quantidade de IPs por rede. Porém, em contrapartida, tornou-se mais fácil pelo fato da existência de protocolos de descoberta de redes (NDP), que permitem, se não corretamente configurados, que atacantes se conectem na rede. Para realizar um *scan* em um número muito grande de hosts da rede pode-se utilizar a ferramenta *alive6* (TEIXEIRA, 2014).

3.2 DoS para novos endereços IPv6 utilizando DAD - (*Duplicate Address Detection* / Detecção de Endereços Duplicados)

O NDP facilitou a comunicação da rede IPv6, mas introduziu falhas que podem gerar vários tipos de ataques. Um deles é o DoS na atribuição de novos IPs. Quando um novo nó quer ingressar numa rede IPv6, é necessário que ele envie uma mensagem *Neighbor Solicitation* para todo enlace, informando o endereço que deseja atribuir para si. Nesse momento, maliciosamente, o atacante envia para o enlace uma mensagem de resposta *Neighbor Advertisiment* informando que está usando o endereço desejado pelo novo nó. A repetição desse processo fará com que o novo nó nunca consiga validar seu IP nem entrar na rede, isolando-o da Internet. Esse ataque é realizado de forma simples e fácil com a ferramenta *dos-new-ip6* (TEIXEIRA, 2014). Também é possível realizá-la com a ferramenta *fake_advertisiment6* (RIBEIRO, 2015).

3.3 *Router Advertisiment Spoofing*

Outra vulnerabilidade advinda do NDP é o *spoofing* de mensagens ICMPv6 *Router Advertisiment*. O nó que envia essa mensagem infoma para o enlace que ele é um roteador da rede. Dessa forma, uma máquina atacante pode se fazer de roteador enviando uma *Router Advertisiment* falsificada, direcionando o tráfego da rede local para o atacante (XAVIER; JUNIOR; MASIN; SILVA, 2012). Com esse *status*, o ataque pode se dar em três abordagens (RIBEIRO, 2015):

- O atacante não permite rota para o exterior deixando a rede isolada da Internet. O atacante recebe o pacote mas não o encaminha, causando um DoS.

- O atacante permite rota para o exterior, liberando o acesso à Internet. O atacante recebe o pacote e o encaminha, configurando um ataque *man-in-the-middle*.

- Ainda, o atacante pode enviar *Router Advertisiments* com o endereço do roteador verdadeiro e com o *lifetime* com o valor 0, indicando que esse roteador não existe mais. Dessa forma, os hosts que receberem essa mensagem excluirão a rota para esse roteador.

Esse ataque é de grau de dificuldade médio e causa grandes danos às vítimas utilizando a ferramenta *scapy6* (RIBEIRO, 2015). A ferramenta *fake_router26* também pode ser usada para este propósito (XAVIER; JUNIOR; MASIN; SILVA, 2012).

3.4 *Flooding* de Mensagens NDP

O ataque tipo *flooding* visa esgotar os recursos do alvo. Nesse caso, o atacante envia inúmeras mensagens NDP *Neighbor Advertisiment*, *Router Advertisiment* ou *Neighbor*

Solicitation para o endereço *multicast* do enlace comprometendo a rede e as máquinas ligadas a ela, pois, com tantas mensagens solicitando informações ou mudanças de configuração, estas ficam sobrecarregadas e entram em estado de negação de serviço. Em especial, o envio massivo de mensagens *Router Advertisiment* faz com que sejam ofertadas várias redes ao alvo e, ao tentar configurar todas ao mesmo tempo, vê sua CPU consumida em 100%, causando a parada do Sistema Operacional. Para este ataque de fácil realização podem ser utilizadas as ferramentas *flood_advertise6* e *flood_router26* (GARCIA; RHODEN; WESTPHALL, 2015). Além da ferramenta *flood_solicitate6* (RIBEIRO, 2015).

Alternativamente, o atacante pode enviar massivamente mensagens SEND. Com a alta taxa dessas mensagens, os nós da rede terão problemas de desempenho já que o processamento de mensagens CGA é muito custoso, podendo causar DoS. A ferramenta *sendpees6* pode realizar este ataque (RIBEIRO, 2015).

3.5 DoS DHCPv6

Analogamente ao ataque para versão DHCPv4, o atacante busca consumir todos os endereços IPs disponíveis na rede. Naturalmente, no IPv6 será mais difícil realizar este ataque, haja vista o elevado número de IPv6 disponíveis, mas, se o administrador da rede tiver definido um pequeno intervalo de endereços, esse ataque funcionará. Combinadas com a atribuição de todos os IPs do intervalo definido, as informações de configuração de cada cliente ficarão armazenadas do servidor DHCP, consumindo sua memória e podendo causar transbordamento (MOREIRAS, 2013). Neste fácil ataque pode-se usar a ferramenta *flood_dhcp6* (RIBEIRO, 2015).

3.6 DoS por Mensagens *Multicast*

Este é outro ataque herdado do IPv4, porém, em vez de serem usadas mensagens *broadcast*, são enviadas mensagens *multicast* de todos os nós local com o endereço de origem da máquina alvo. Ao receberem as mensagens, todos os nós enviam respostas para o alvo ampliando seu tráfego e exaurindo seus recursos. Com o uso da ferramente *smurf6* este ataque é realizado de maneira simples (TEIXEIRA, 2014).

4 MÉTODOS DE DETECÇÃO E DEFESA

Inicialmente, numa rede potencialmente insegura, faz-se necessário a realização de uma análise de riscos visando a implantação de medidas de segurança para baixar ou eliminar

a possibilidade de exploração das vulnerabilidades da rede. Assim, serão enumeradas algumas dessas medidas para cada uma das vulnerabilidades citadas com intenção de saná-las.

4.1 Reconhecimento da Rede

Como este procedimento não se trata especificamente de um ataque, não existe solução pronta. No entanto, alguns mecanismos podem ser ativados e outros desativados para que a varredura da rede seja insatisfatória ou, até mesmo, não se realize. Por exemplo (RIBEIRO, 2015):

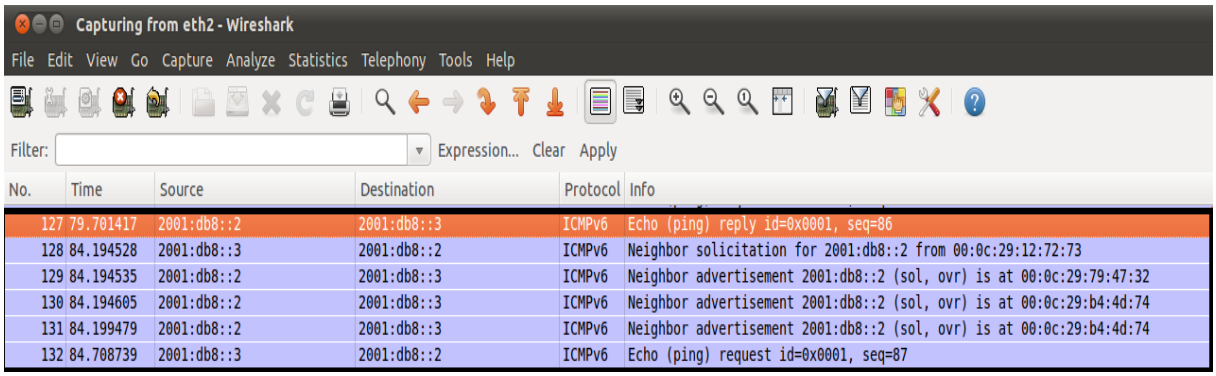
- A autoconfiguração automática de endereços deve ser evitada. Em alternativa, deve-se usar o SEND, devido a CGA;
- Na utilização do DHCPv6, o *range* de IPs a serem distribuídos não deve começar nos primeiros endereços de nós disponíveis;
- Atribuição de endereços de maneira aleatória.

Com a habilitação do IPSEC (com autenticação por certificado, palavra-chave, etc) e de regras de *firewall* (permitir respostas ICMP somente se for de trafego seguro) também podemos evitar o *scan* da rede (TEIXEIRA, 2014).

4.2 DoS para novos endereços IPv6 utilizando DAD - (*Duplicate Address Detection* / Detecção de Endereços Duplicados)

Para detectar esse ataque, captura e análise tráfego se fazem necessárias para diferenciação do tráfego legítimo do ilegítimo. A ferramenta mais difundida para isso é o *Wireshark*. Um exemplo de detecção é mostrado na Figura 2, onde podem se verificar as mensagens *Neighbor Advertisiment* falsas.

Figura 2: Momento da detecção de mensagens *Neighbor Advertisiment* falsas com a ferramenta *Wireshark*.



Fonte: (TEIXEIRA, 2014)

Adicionalmente, a ferramenta *6Guard* realiza detecção de ataques de mascaramento de pacotes (GARCIA; RHODEN; WESTPHALL, 2015). Também, a ferramenta NDPMon é usada em redes IPv6 para monitoramento de mensagens ICMPv6, buscando irregularidades em mensagens NDP. O NDPMon é uma ferramenta passiva: não realiza reações às suas detecções, apenas efetua registros em logs do sistema e alertas para o administrador de rede (XAVIER; JUNIOR; MASIN; SILVA, 2012). Em termos de impedimento desse ataque, a combinação do SEND com o IPSEC diminui a quase zero o poder desse ataque (TEIXEIRA, 2014).

4.3 *Router Advertisiment Spoofing*

Para dificultar a aceitação de mensagens *Router Advertisiment* ilícitas é necessário fixar requisitos para que estas sejam aceitas. Também, convém que as mensagens *Router Discovery* sejam descartadas delegando o serviço de prestar informações da rede ao servidor DHCPv6, caso presente na rede. O uso do IPSEC e do SEND também se faz aconselhável (RIBEIRO, 2015).

Para inibir esse ataque deve-se utilizar a ferramenta *RA Guard* que permite ao administrador da rede rejeitar mensagens *Router Advertisiment* indesejadas, ou seja, que foram emitidas por equipamentos não autorizados. É um mecanismo previsto na RFC 6105 que preconiza que mensagens *Router Advertisiment*, que chegam ao *switch* por portas diferentes da do roteador, devem ser descartadas (XAVIER; JUNIOR; MASIN; SILVA, 2012).

4.4 *Flooding* de Mensagens NDP

Analogamente à defesa do ataque anterior, a filtragem de mensagens *Router Advertisiment* e *Router Discovery* devem ser implantadas. O IPSEC, o SEND e o *RA Guard*

também são imprescindíveis para a defesa (GARCIA; RHODEN; WESTPHALL, 2015). No caso do *flooding* de mensagens SEND, se o sistema não possuir boa capacidade de processamento, o SEND deve ser desabilitado para evitar o risco de degradação de serviços a níveis indesejados. Nesse cenário, é necessario que se faça o estudo para cada rede, decidindo se é menos pior ficar exposto a *flooding* SEND ou a *flooding* NDP (RIBEIRO, 2015).

4.5 DoS DHCPv6

Para limitar requisições DHCP a ferramenta *Port Security* pode ser utilizada, pois restringe a uma determinada quantidade de mensagens DHCP por cada porta do *switch*. Em redes sem fio, a *Port Security*, talvez, não seja recomendada devido a imprevisibilidade do número de acessos à rede. Em alternativa, tem-se a ferramenta *DHCP Snooping* que bloqueia pacotes DHCP por porta (RIBEIRO, 2015).

4.6 DoS por Mensagens *Multicast*

Este tipo de DoS é difícil de ser detectado e rastreado. Como possível resolução deste ataque temos a adição de regras no *firewall* como o bloqueio de mensagens ICMP para endereços de *multicast* e bloqueio de pacotes com endereços de origem não pertencentes à rede ligada a determinada interface do roteador/*firewall* (TEIXEIRA, 2014).

5 CONSIDERAÇÕES FINAIS

A nova versão do protocolo IP (IPv6), inicialmente concebida para sanar o problema do esgotamento de endereços IPv4, trouxe muitas outras funcionalidades com o objetivo de torná-lo mais enxuto e mais seguro. A adição dessas novas funcionalidades no IPv6 demandou mais atenção dos administradores de rede para enfrentar os desafios de sua implantação, pois foram constatadas algumas vulnerabilidades, devido a este protocolo ainda não se encontrar em fase madura.

Assim, a análise de riscos da infraestrutura da rede faz-se de grande valia para detectar as vulnerabilidades, enumerar contramedidas para eliminar ou mitigar efeitos causados pela exploração e elaborar planos e políticas de segurança da informação de acordo com a legislação vigente, visando disseminar conhecimento acerca do novo protocolo para gerentes da rede e usuários.

Visando isso, este trabalho busca ser um insumo para os administradores de rede realizarem suas análises de riscos e políticas de segurança da informação, estudando como

algumas das novas vulnerabilidades do IPv6, escolhidas pela facilidade de exploração e dimensão do dano causado à vítima, são exploradas e como as ferramentas de detecção e defesa agem para tentar eliminá-las, enumerando-as.

Dessa forma, as vulnerabilidades foram apresentadas explicando seus problemas, como os do NDP, que facilita a entrada de atacantes na rede, e foram sugeridas ferramentas de detecção e eliminação, como o *WireShark* e a *RA Guard*, além dos imprescindíveis IPSEC e SEND, que, sozinhos, eliminam parte significativa das ameaças.

Mesmo com a eficiência comprovada dessas ferramentas, outros mecanismos devem ser usados em conjunto, como RADIUS com o padrão IEEE 802.1X (TEIXEIRA, 2014). Algumas modalidades de vulnerabilidades ficaram fora do escopo desse trabalho, como as vulnerabilidades de transição IPv4/IPv6, mas que de forma alguma devem ser ignoradas, bem como aquelas que independem de protocolo como vírus, homem-do-meio e DoS.

Naturalmente que, com o crescimento e disseminação do uso do IPv6, novas vulnerabilidades aparecerão e a vigilância há que ser constante para se manter atualizado com as novas medidas de segurança em reposta a essas novas ameaças, como por exemplo sistemas IDS e IPS.

REFERÊNCIAS

BEIRA, Henrique Gonçalves. Método e análise de desempenho e segurança de uma rede IPv6 utilizando IPSec em modo túnel. Curitiba - PR. 2014.

CAMACHO, Flávio Gomes Figueira. Segurança com IPv6. Niterói - RJ. 2012.

COAN, Anderson Luiz. Implementação do protocolo IPV6 com segurança: Uma análise sobre os desafios e riscos para os administradores de redes internet. São Paulo - SP. 2013.

GARCIA, Eduardo de Mello; RHODEN, Guilherme Eliseu; WESTPHALL, Carla Merkle. Elaboração e realização de experimentos de segurança em cenários de transição IPv4/IPv6. In: XV SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS - SBSeg 2015. Anais. Florianópolis. p. 427-436.

IPV6.BR. Disponível em <http://www.ipv6.br/>. Acessado em 04/2016.

MOREIRAS, Antonio M. Desafios do IPv6 para profissionais de segurança. In: 2o. FÓRUM BRASILEIRO DE CSIRTS - Grupos de Segurança e Resposta a Incidentes. São Paulo - SP. 2013.

RIBEIRO, André Filipe Costa. IPv6 – Integração, transição e segurança. 2015. Dissertação (Mestrado em Ciências). Instituto Superior de Engenharia do Porto. Porto. Portugal.

SIQUEIRA, Alessandro Nucci. Redes IPv6 e estratégias de implementação. São Paulo - SP. 2011.

TEIXEIRA, Fabiano de Assis. Medidas de segurança para as principais vulnerabilidades do protocolo IPv6. Serra - ES. 2014.

TUVO, Rafael Pimenta. Comparação da segurança nativa nos protocolos IPv4 e IPv6. Salvador - BA. 2011.

XAVIER, Christopher Breno Coelho; JÚNIOR, José Fernando Almeida Teobaldo; MASIN, David Teixeira de; SILVA, Fernando Ramiro Lavor Chacon e. Ferramentas para prevenção e monitoramento de ataques DoS em redes IPv6. Fortaleza - CE. 2012.