FACULDADE ANGLO-AMERICANO DE FOZ DO IGUAÇU

LEANDRO SOLAGNA
MATHEUS FELIPE BONETTI CASTEGNARO

ESTUDO SOBRE SEGURANÇA EM REDE DE COMPUTADORES DOMÉSTICAS UTILIZANDO PROTOCOLOS DE SEGURANÇA

FOZ DO IGUAÇU

2016

LEANDRO SOLAGNA
MATHEUS FELIPE BONETTI CASTEGNARO

ESTUDO SOBRE SEGURANÇA EM REDE DE COMPUTADORES DOMÉSTICAS UTILIZANDO PROTOCOLOS DE SEGURANÇA

Trabalho de conclusão de curso apresentado como requisito obrigatório para obtenção do título de Bacharel em Ciência da Computação da Faculdade Anglo-Americano de Foz do Iguaçu.

Orientador: Prof. Esp. João Paulo de Lima Barbosa

FOZ DO IGUAÇU

2016

"Eu enfrento leões.
Nado com os tubarões.
Se por ventura cair, já estou de pé. (Drawtheline)

RESUMO

Esse trabalho tem como objetivo, avaliar se os equipamentos de redes domésticas atuais, possuem suporte aos protocolos SEND e RA Guard. O estudo de caso, apresentará as características de cada protocolo, assim como o seu funcionamento e protocolos que trabalham em conjunto. Demonstrando também, a importância de se ter segurança mesmo que a rede de computadores seja pequena.

Palavras-chaves: SEND, RA Guard, IPv6, Segurança.

ABSTRACT

This project has as a goal, the evaluation of small offices network equipaments when it comes to security. As for that, it will be through SEND and RA Guard protocols, as if these equipaments have any sort of support to these security protocolos. It will also be studied, their characteristics, how they work and other protocols that work together. This study will also show how important is to have network security, even for a small office.

Keywords: SEND, RA Guard, IPv6, Security.

LISTA DE ABREVIATURAS

UCLA	*University of California, Los Angeles* - Universidade da Califórnia, Los Angeles[1]
SIR	*Stanford Research Institute* - Instituto de Pesquisa *Stanford*[1]
IP	*Internet Protocol* - Protocolo de Internet[1]
IPv4	*Internet Protocol version 4* - Protocolo de Internet versão 4[1]
CIDR	*Classless Inter-Domain Routing* - Roteamento Intra Domínio Sem Classe[1]
NAT	*Network Address Translation* - Tradução de Endereço de Rede[1]
IPv6	*Internet Protocolo version 6* - Protocolo de Internet versão 6[1]
ICMP	*Internet Control Message Protocol* - Protocolo de Controle de Mensagem da Internet[1]
DHCP	*Dynamic Host Configuration Protocol* - Protocolo de Configuração Dinâmica de Host[1]
IPSec	*IP Security Protocol* - Protocolo de Segurança[1]
ARP	*Address Resolution Protocol* - Protocolo de Resolução de Endereço[1]
RARP	*Reverse Address Resolution Protocol* - Protocolo de Resolução Reversa de Endereços[1]
IGMP	*Internet Group Management Protocol* - Protocolo Gerenciamento de Grupos da Internet[1]
ICMPv6	*Internet Control Message Protocol version 6* - Protocolo de Controle de Mensagem da Internet versão 6[1]
RS	*Router Solicitation*
RA	*Router Advertisement*
NA	*Neighbor Solicitation*
NS	*Neighbor Advertisement*

[1] Tradução dos autores

MAC	*Media Access Control* - Controle de Acesso à Mídia[1]
NDP	*Neighbor Discovery Protocol* - Protocolo de Descoberta de Vizinhança[1]
SEND	*SEcure Neighbor Discovery*
RA Guard	*Router Advertisement Guard*
DARPA	*Defense Advanced Research Projects Agency*
ARPANET	*Advanced Research Projects Agency Network*
OSI	*Open System Interconnection model*
TCP	*Transmission Control Protocol*
NAT	*Network Address Translation*
IANA	*Internet Assigned Numbers Authority*
ICAN	*Internet Corporation for Assigned Names and Numbers*
RIR	*Regional Internet Registries* - Registro Regional da Internet
LACNIC	*Latin America and Caribbean Network Information* - Registro de Endereçamento da Internet para América Latina e Caribe

SUMÁRIO

1 INTRODUÇÃO

O crescimento contínuo e global da Internet é um dos fenômenos mais interessantes e excitantes em redes. Há algumas décadas, não se imaginava que um projeto de pesquisa envolvendo duas universidades da Califórnia – UCLA (Universidade da Califórnia, Los Angeles) e SRI (Instituto de Pesquisa Stanford), se tornaria o principal meio de comunicação no dia a dia das pessoas.

Para que essa comunicação aconteça, protocolos que ditam as regras de conexão, entre uma origem e destino, foram criados. Ou seja, possibilitando assim a comunicação entre pessoas ou máquinas, não importando a sua localização global. Entre vários protocolos que foram criados, o mais importante foi, o IP (Protocolo de Internet). O IP é responsável por dar um endereço único para cada dispositivo conectado em uma rede de computadores, permitindo assim, que as informações cheguem ao seu destino (ALECRIM, 2011).

A partir de 1983, a Internet começou a usar o IP versão 4 (IPv4). Isto fez com que a rede mundial de computadores crescesse em um ritmo acelerado, com vários equipamentos sendo criados e necessitando de um endereço único para funcionar normalmente. Por causa disso, cientistas e especialistas perceberam no final da década de 80, que os números de IPv4 estavam próximos de esgotarem (MOREIRAS, 2014).

Dessa forma, começaram pesquisas para se encontrar uma solução adequada para esse problema. Nos anos 90, solução como o CIDR (Roteamento Intra Domínio Sem Classe) foi proposto, com o intuito de usar os endereços IPs de forma mais eficiente. Em tempos mais recentes, começo dos anos 2000, o NAT (Tradução de Endereço de Rede) foi proposto, mascarando IPs inválidos para que os usuários possam acessar a nuvem. Obviamente, essas soluções só foram propostas como temporárias, o grande problema ainda existia, o limite de endereços IPv4. A solução proposta foi a atualização do protocolo, usado na época, para um outro que pudesse gerar mais endereços únicos. Foi então desenvolvido o IP versão 6 (IPv6). Nessa versão, a característica principal foi o aumento de número de endereços, passando de 4 bilhões para mais de 340 undecilhões (NIC.BR, 2012).

Os cientistas aproveitaram essa oportunidade para mudar outras características do protocolo, algumas dessas foi a alteração do cabeçalho para um menos complexo de se entender, protocolos que auxiliam o IPv6 no seu funcionamento, ICMP (Protocolo de Controle de Mensagem da Internet), DHCP (Protocolo de Configuração Dinâmica de Host) e IPSec (Protocolo de Segurança) também foram modificados.

Assim como na versão anterior, o IPv6 usa o protocolo de controle de mensagens da Internet ICMP, que tem como responsabilidade enviar mensagens de erro indicando que o serviço, roteador ou um endereço de rede está indisponível. No IPv6, além de reportar erros no processamento de pacotes, realizar diagnósticos e enviar mensagens sobre as características da rede, o protocolo ICMPv6 assumiu também funcionalidades dos protocolos ARP (Protocolo de Resolução de Endereço), RARP (Protocolo de Resolução Reversa de Endereços) e IGMP (Protocolo Gerenciamento de Grupos da Internet) (TELECO, 2011).

Os protocolos ARP e RARP, em geral, são utilizados para encontrar um endereço único em um dispositivo em uma rede. O protocolo IGMP tem como função controlar os membros de um grupo de *multicast*.

Com o ICMPv6 (Protocolo de Controle de Mensagem da Internet versão 6), várias mensagens são trocadas em uma rede local, sendo quatro delas fundamentais para a descoberta de hosts IPv6 vizinhos:

- RS (*Router Solicitation*): mensagem enviada de uma estação que deseja aprender informações de um roteador de uma rede local;
- RA (*Router Advertisement*): mensagens enviadas em respostas às mensagens RS, podendo também ser usada para enviar anúncios não solicitados para toda a rede, informando da sua existência;
- NS (*Neighbor Solicitation*): mensagem enviada por uma máquina com o objetivo de encontrar o endereço MAC (Controle de Acesso à Mídia) de um endereço IPv6;
- NA (*Neighbor Advertisement*): São respostas à mensagens NS ou para informar a mudança de endereço de uma máquina.

Com o protocolo ICMP atualizado, um novo protocolo dependente do ICMP foi criado, o NDP(Protocolo Descoberta de Vizinhança). O NDP do ICMPv6 permite saber quais são as máquinas da rede, encontrar roteadores vizinhos, detectar endereços duplicados e detectar outras anomalias que possam acontecer dentro de uma rede de computadores (NARTEN E. NORDMARK, 2007).

O protocolo IPv6 ainda é considerado um protocolo novo, por isso, suas vulnerabilidades ainda não foram exploradas ao máximo (POULIN, 2014).

Assim como no seu antecessor (IPv4), o IPv6 possui vulnerabilidades que podem ser exploradas através de ataque como *man-in-the-middle*, cujo objetivo é o roubo de informações ou ataques que possam negar algum serviço, fazendo com que o usuário da rede não consiga utilizá-la.

Para fornecer segurança contra ataques que possam se passar por uma máquina ou um dispositivo da rede foi criado uma extensão do protocolo NDP, chamado de SEND (*SEcure Neighbor Discovery*). Este protocolo propõe solução aos seguintes itens (ARKKO ED. ERICSSON, 2005):

- Criação de uma cadeia de certificados;
- A utilização de endereços gerados criptograficamente;
- Criação de opções para proteger todas as mensagens relativas ao NDP;
- Prevenir ataques de reenvio de mensagens por meio de duas novas opções no NDP;

Quando se usa o IPv6, sem o apoio do SEND em todos os dispositivos da rede, há sempre o risco de lidar com problemas que envolvem o envio indevido dos RA, que são mensagens enviadas por roteadores em resposta às mensagens de requisitos ou RS, por roteadores não autorizados ou indevidamente configurados na rede (TELECO, 2011).

Uma alternativa para esse problema é o protocolo RA Guard (*Router Advertisement Guard*), que surgiu devido à dificuldade de implementação do SEND.

O IPv6 RA Guard monitora mensagens de RA originadas de um roteador não autorizado. Esse protocolo analisa as RA e filtra as mensagens de dispositivos não autorizados, através de uma tabela, que possui as informações dos roteadores autorizados na rede. citar: https://tools.ietf.org/html/rfc6105

Essa técnica é usada para ajudar o administrador a identificar ataques como *man-in-the-middle*, um roteador da rede que não está autorizado e negação de serviço por configuração inválida (HOGG, 2014).

1.1 JUSTIFICATIVA

Atualmente, existem métodos com o objetivo de roubar informações. Alguns destes métodos podem ser utilizados para, ao infiltrar-se, se passar por um roteador ou uma máquina na rede, visando ter o tráfego da rede passando por eles, dessa forma, obtêm-se pacotes contendo informações sigilosas.

Com o intuito de evitar esses possíveis ataques, os protocolos SEND e RA Guard foram criados para que uma ação e um alerta ocorram no momento em que se detecta uma invasão dentro de uma rede.

Nos dias atuais, é necessário saber se os dispositivos de redes domésticas vendidos no mercado suportam no mínimo um desses protocolos.

1.2 OBJETIVOS

Nesta sessão serão abordados os objetivos gerais e específicos deste trabalho. Apresentando os pontos de interesse, no qual almeja-se chegar ao fim do projeto aqui apresentado.

1.2.1 Objetivo Geral

Descobrir quais atuais equipamentos de uma rede de porte pequeno, possuem suporte aos protocolos de segurança SEND e RA Guard. Para isso, haverá a necessidade de implementar esses protocolos e testá-los nos equipamentos instalados. Por fim, uma tabela com os dispositivos testados será apresentado, nela, constará os resultados obtidos durante os testes.

1.2.2 Objetivos Específicos

- Pesquisar sobre os funcionamentos dos protocolos SEND e RA Guard, assim como os protocolos de IPv6 que trabalham junto a eles.
- Montar um ambiente de testes, com equipamentos atuais, para que os protocolos pesquisados possam ser colocados em prática.
- Inserir os protocolos de proteção no ambiente de testes, para que possam ser demonstrados.
- Através de uma tabela comparativa, apresentar quais os dispositivos atuais que possuem suporte para as técnicas de proteção abordadas.

1.3 ORGANIZAÇÃO DO TRABALHO

Esta sessão, apresentará uma breve descrição dos capítulos presentes neste trabalho. No capítulo 2, serão descritos os fundamentos teóricos, com a finalidade de compreender o tema proposto. Temas como funcionalidades do IPv4, IPv6, segurança, ameaças e vulnerabilidades serão mostrados

No capítulo 3, são apresentados os protocolos de segurança SEND e RA Guard e abordado a sua funcionalidade e seus componentes.

No capítulo 4, apresentam-se as formas de implementações, equipamentos necessários para isso, equipamentos das quais serão testados e definições necessárias para o entendimento acerca do tema abordado neste trabalho.

No capítulo 5, apresentam-se os resultados obtidos com o desenvolvimento do projeto de forma geral.

No capítulo 6, a conclusão e trabalhos futuros são abordados.

2 REVISÃO BIBLIOGRÁFICA

O inicio das redes de computadores aconteceu nos Estados Unidos, onde pesquisadores do DARPA (*Defense Advanced Research Projects Agency*) começaram a experimentar com comunicação entre computadores, onde perceberam o potencial de uma rede de computadores que utilizam pacotes para se comunicarem.

Após esses experimentos a ARPANET (*Advanced Research Projects Agency Network*) foi criada tendo como primeiro nó a UCLA e o segundo nó a SRI, onde receberam a primeira mensagem de nó-a-nó (LEINER V. CERF,).

Isso tudo levou a adição de vários outros nós à rede. Infelizmente, os problemas começaram a surgir, ficando claro que seria necessário desenvolver protocolos para maior garantia de comunicação entre todos os nós.

Em razão disso, protocolos como o IPv4 foram desenvolvidos.

Com o esgotamento do número endereços IPv4 mais próximo a cada dia, tecnologias começaram a ser desenvolvidas para o IPv6. Iniciou-se pesquisa para extensões de protocolos, novos protocolos foram criados e tecnologias que utilizam IPv6 tiveram maior foco.

Dentro de várias pesquisas, surgiram duas para segurança em redes que utilizam o IPv6, das quais deram inspirações nesse trabalho. Cujo foco é saber se equipamentos de redes domésticas possuem suporte para protocolos de segurança em rede.

Não é possível falar de IPv6 e suas tecnologias, sem mencionar o seu antecessor.

2.1 IPv4

A primeira versão do protocolo de Internet a ser utilizada globalmente. Trabalha na camada de rede do modelo OSI (*Open System Interconnection model*) e na camada de Internet no modelo TCP (*Transmission Control Protocol*)/IP.

Responsável por indentificar hospedeiros onde providencia um endereço único para cada hospedeiro em uma rede.

O cabeçalho deste protocolo contem 14 campos, da qual cada um possui a sua obrigação.

Com suporte a três tipos diferentes de modos de endereçamento, da qual se chamam *unicast*, *broadcast* e *multicast*.

O protocolo divide cada endereço em uma hierarquia de dois níveis, prefixo e sufixo, o prefixo de um endereço identifica a rede a qual o dispositivo se liga, e o sufixo identifica um dispositivo específico na rede. Um endereço de IP é um número de 32 bits. No início, o endereço pertencia a uma de cinco classes, em que a classe de um endereço era determinada pelo valor dos quatro primeiros bits, onde a uma rede física que contivesse entre 257 e 65.536 hospedeiros era atribuído o valor de prefixo B. As redes menores era atribuído um valor prefixo de classe C, e as redes maiores era atribuído o prefixo de classe A. (Refe: Livro do joão, usado nas aulas de redes)

Apesar disso, existem endereços reservados para uso pessoal.

Toda a classe de IP's possui endereços reservados que podem ser utilizados em uma rede local, por exemplo, em empresas e em casas. Esses endereços podem ser chamados de IPv4 inválidos, pois não são roteaveis na Internet.

Em razão disso foi desenvolvido a tecnologia NAT (*Network Address Translation*), que faz a tradução de um IP inválido para IP válido. Basicamente o NAT pega o seu endereço inválido e o mascara utilizando o único IP válido que a pessoa possui. Dessa forma, a rede externa acredita que o usuário está utilizando aquele IP válido para acessar páginas *web*.

Para receber um endereço IP, o computador procura um servidor DHCP, se houver um na rede, um endereço é atribuído. Outra alternativa é configurar manualmente um endereço IP para que então o computador possa se comunicar com outros na rede.

A alocação de IPv4 é globalmente gerenciada pela IANA (Internet Assigned Numbers Authority) em coordenação com a ICANN (Internet Corporation for Assigned Names and Numbers). A IANA trabalha junto com os cincos RIRs (Registro Regional da Internet) existentes. Na américa latina o orgão responsável por entrega de endereços IPv4 válidos é a LACNIC (Registro de Endereçamento da Internet para América Latina e Caribe).

2.2 IPv6

REFERÊNCIAS

ALECRIM, E. **Endereço IP (Internet Protocol)**. 2011. Acesso em 26 de maio de 2016. Disponível em: <http://www.infowester.com/ip.php>.

ARKKO ED. ERICSSON, J. K. B. Z. P. N. J. **SEcure Neighbor Discovery (SEND)**. 2005. Acesso em 27 de maio de 2016. Disponível em: <https://tools.ietf.org/html/rfc3971>.

HOGG, S. **Why You Must Use ICMPv6 Router Advertisements (RAs)**. 2014. Acesso em 27 de maio de 2016. Disponível em: <https://community.infoblox.com/t5/IPv6-Center-of-Excellence/Why-You-Must-Use-ICMPv6-Router-Advertisements-RAs/ba-p/3416>.

LEINER V. CERF, D. C. R. K. L. K. D. L. J. P. L. R. S. W. B. **Brief History of the Internet**. Acesso em 01 de junho de 2016. Disponível em: <http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet>.

MOREIRAS, A. **IPv6, um desafio técnico para a Internet**. 2014. Acesso em 26 de maio de 2016. Disponível em: <http://cio.com.br/tecnologia/2014/02/04/ipv6-um-desafio-tecnico-para-a-internet/>.

NARTEN E. NORDMARK, W. S. H. S. T. **Neighbor Discovery for IP version 6 (IPv6)**. 2007. Acesso em 27 de maio de 2016. Disponível em: <https://tools.ietf.org/html/rfc4861>.

NIC.BR. **Endereçamento**. 2012. Acesso em 26 de maio de 2016. Disponível em: <http://ipv6.br/post/enderecamento/>.

POULIN, C. **The Importance of IPv6 and the Internet of Things**. 2014. Acesso em 27 de maio de 2016. Disponível em: <https://securityintelligence.com/the-importance-of-ipv6-and-the-internet-of-things/>.

TELECO. **Rede IP I: Fundamentação Teórica**. 2011. Acesso em 26 de maio de 2016. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialredeipmig1/pagina_2.asp>.