Análise da Segurança em Redes Puramente Ipv6

Luis Godinho Júnior[1], Jarbas Pereira Lopes Sousa[1], Robert Mady Nunes[1], Madianita Bogo[1]

[1]Curso de Sistemas de Informação – Centro Universitário Luterano de Palmas (CEULP/ULBRA)
Teotônio Segurado 1501 SUL – 77054-970 – Palmas – TO – Brasil

luisgodinhojr@hotmail.com, {jarbas, robert, madia}@ulbra-to.br

RESUMO: *Um dos grandes problemas na comunicação na Internet é a necessidade de garantia de segurança das informações. O novo protocolo de rede da Internet, o IPv6, entre outras características, visa oferecer maior segurança mandatária, utilizando o IPSec. Como é um tema que ainda está em fase de estudos, ainda existe muito a ser explicado. Assim, esse trabalho tem como foco analisar a segurança do novo protocolo da Internet, o ipv6, abordando um estudo teórico e testes de comunicação em uma rede puramente IPv6.*

1. Introdução

Desde o seu surgimento a *Internet* cresceu muito, tanto na utilização domiciliar quanto nas empresas, desta forma cresceram o número de *intranets*, que estão ligadas a outras *intranets* e *extranets*. Junto com esse crescimento aumentou, também, a necessidade de garantir a segurança na comunicação, já que vários tipos de transações ocorrem via *Internet*. Os dados trafegados pela rede podem ser capturados, pois há vários programas de captura que podem ser usados na rede para pegar as mensagens, e até alterados.

O protocolo responsável pela comunicação dos dados na *Internet* é o IP, atualmente na versão 4. Devido ao crescimento da *Internet*, nos anos 90 iniciou-se o projeto da versão 6 do protocolo – IPv6 (*Internet Protocol version 6*) – que fornece um maior espaço de endereçamentos que a versão atual e sugere algumas melhorias, como a segurança mandatária, que não era prevista no IPv4.

A idéia é que a garantia de segurança não dependa da configuração do usuário e seja oferecida em todas as redes, como o protocolo IPSec. O protocolo IPSec visa garantir essa segurança oferecendo serviço de autenticação e/ou criptografa na camada de rede. No entanto, não foram encontrados resultados de testes nem documentos que mostrem como os desenvolvedores dos Sistemas Operacionais Windows e Linux implementam as funcionalidades especificadas e se o IPSec já está habilitado como padrão, quando se usa o IPv6**.**

Assim, o objetivo desse trabalho é realizar uma análise da segurança de redes puramente IPv6, em ambiente Linux e Windows, verificando se esses Sistemas Operacionais oferecem segurança por padrão, conforme é a proposta do protocolo, sem que haja necessidade de configurações extras por parte dos usuários.

GODINHO JR, Luis; SOUSA, Jarbas Pereira Lopes; NUNES, Robert Mady, BOGO, Madianita. Análise da Segurança em Redes Puramente Ipv6. In: VII ENCONTRO DE ESTUDANTES DE INFORMÁTICA DO ESTADO DO TOCANTINS, 2005, Palmas. **Anais...** Palmas: 2005.

2. Protocolo IPv6

Desde os anos 70 utiliza-se o protocolo IP para a comunicação em rede e a partir do início dos anos 80 o IPv4, versão atual do protocolo, passou a ser um dos protocolos mais utilizados no mundo [Obelheiros, 1999]. Com o passar do tempo e com a possibilidade da falta de endereços a IETF organizou um grupo de desenvolvimento para a criação de um novo protocolo, o IPv6. Este protocolo mantém as principais características que fizeram do IPv4 um sucesso mundial, como o fato de não ser baseado em conexão e deixar a confiabilidade para os protocolos de mais alto nível. Porém, além de ampliar o espaço de endereçamento, dar segurança na conectividade, o IPv6 acrescenta novas funcionalidades ao IPv4 e altera algumas características, que são:

- Simplificação do cabeçalho: vários campos presentes no IPv4 foram suprimidos e outros tornaram–se opcionais [Martins, 2000]. Um cabeçalho mais simplificado implica em menos processamento para cada pacote, sendo extremamente útil para redes de alta velocidade.
- Cabeçalhos de extensão: são inseridos ao cabeçalho base para prover alguns serviços importantes, porém irrelevantes para uma simples troca de informações entre *host*s. A forma flexível com que esse cabeçalho foi implementado permite que sejam incluídas novas funcionalidades no futuro.
- Endereçamento de 128 bits: os endereços IPv6 são formados por 128 bits de comprimento, contra os atuais 32 do IPv4, o que aumenta exponencialmente a capacidade de máquinas conectadas;
- Novo formato de endereço: o IPv4 agrupa seus bits em octetos e os representam em decimal, enquanto que o IPv6 agrupa seus bits em oito hexatetos em hexadecimal;
- Rota definida na origem: no IPv4 a rota que era definida durante o envio, na nova versão, passa a ser definida na origem, o que diminui os custos de processamento dos roteadores;
- Suporte a autoconfiguração: permite atribuir automaticamente um endereço IP a um host, o que elimina a necessidade de se configurar manualmente os equipamentos conectados a rede.
- Suporte a endereços *anycast*: no IPv6 foi inserido o endereço *anycast*, que se assemelha a uma junção dos endereços *multicast* e *unicast*. Porém, este suporte ainda está em fase experimental e só poderá ser utilizado por roteadores e nunca por estações clientes.
- Roteamento: tem a função de determinar a rota que os pacotes irão percorrer para alcançar seu destino. Essa rota é definida na origem, diminuindo a carga de trabalho dos roteadores intermediários.

3. Segurança em Redes de Computadores

Devido à praticidade da *Internet*, empresas e industrias resolveram compartilhar informações com seus clientes, parceiros e fornecedores respectivamente. Isso gera um

tráfego ininterrupto na rede e conseqüentemente expõem as informações, a ataques e cópias indevidas.

Para garantir a segurança na comunicação devem-se usar mecanismos lógicos para prover uma determinada proteção aos dados, controlando acessos, utilizando detecção de intrusos, criptografia de dados, entre outros mecanismos de proteção. Além disso, espera-se que a proteção ao acesso físico não seja deixada de lado, pois toda a segurança lógica pode cair por terra. O acesso físico (onde estão dispostos os *hosts*), principalmente os servidores de aplicações de riscos, deve ser permitido a poucas pessoas e deve ser controlado, por exemplo, deve-se registrar cada acesso (com nome, data e hora). Esta medida pode evitar que informações vazem ou sejam manipuladas inadequadamente por algum funcionário autorizado.

Voltando aos mecanismos lógicos, o IPv4 não oferece, por padrão, segurança aos dados em nível de rede. Os dados podem ser facilmente capturados, por *snniffers* (*scanners* de rede*),* que são programas destinados à captura de datagramas que estão trafegando na rede, permitindo a visualização dos dados. Além disso, os sistemas podem sofrer ataques, que são acessos indevidos ao sistema, em que o invasor poderá capturar, alterar ou destruir as informações [SILVA, 2003]. Alguns ataques são:

- *Spoofing*: personificação de endereço IP, o que permite que um *host* qualquer possa se passar por outro, modificando o endereço IP do *host* origem;
- *DOS-DDOS*: negação de serviço. Por causa da sobrecarga ocasionada pela repetição de alguma solicitação, o servidor ("alvo") é forçado a parar o serviço que disponibiliza.

Existem várias formas de evitar esse tipo de problema, sendo que os mecanismos de segurança fornecem serviços como:

- *Autenticidade*: confirma a identidade da outra parte (entidade) envolvida na comunicação;
- *Confidencialidade/Privacidade*: restringe ao remetente e ao destinatário o entendimento da mensagem, pois somente estes podem decifrá–la;
- *Não–repúdio*: impede que uma entidade envolvida em uma comunicação negue a sua participação no evento;
- *Integridade*: garante que a informação não sofreu alterações durante seu percurso na rede.

Para que estes serviços possam ser garantidos é necessário que as informações sejam codificadas (cifradas) e/ou resumidas digitalmente (*Hash*), garantindo a confidencialidade e a integridade respectivamente [Brocardo, 2001].

Para codificar, ou criptografar, deve-se usar algoritmo específicos, que apresentam as opções e variantes de Sistema de Criptografia. Um Sistema de Criptografia possui a finalidade de cifrar, ou criptografar, uma mensagem através de um método de cifragem, ou encriptação. Nestes sistemas, a entrada da mensagem original (texto plano) mais uma chave (senha), que são passados para o sistema de criptografia, resultam na mensagem cifrada, que é então armazenada em um meio qualquer ou transmitida até um receptor [Galiano,1997]. O processo de decifragem é o processo inverso da cifragem.

De acordo com a utilização das chaves, os sistemas de criptografia podem ser classificados como:

- *Simétricos*: Os sistemas simétricos utilizam uma única chave para encriptação e decriptação, que deverá ser mantida sob sigilo, sendo conhecida apenas pelos envolvidos na troca de mensagens. Os principais sistemas simétricos são: DES, 3DES, RC2, RC4 e RC5;
- *Assimétricos*: Os sistemas assimétricos, conhecidos também como sistemas de chave pública, utilizam um par de chaves, sendo uma de uso privado, que é mantida em sigilo pelo usuário, e outra de uso público, que pode ser acessada por qualquer pessoa. As chaves são diferentes e a partir de uma não se pode chegar à outra. Os dois principais sistemas de criptografia de chave pública são: DH (*Diffie Hellman*), RSA.

Como foi citado anteriormente, um dos serviços de segurança é a integridade, que tem por objetivo verificar que a informação não foi modificada indevidamente. A integridade pode ser garantida através de uma técnica de resumo digital, chamada de funções *Hash*.

Uma função *Hash* pode ser comparada a uma impressão digital. Da mesma maneira que uma impressão digital identifica exclusivamente um individuo, uma função *Hash* calcula um valor de identificação para a mensagem [Puttini, 2003]. Quando se aplica uma função *Hash* em uma mensagem M (*Hash*(M)) é retornado um valor inteiro. Assim, para verificar se houve alteração na mensagem basta calcular o *Hash* da recebida e compará-lo com o da mensagem original, se forem iguais significa que a mensagem está intacta.

4. IPSec

Quando o IPv4 foi desenvolvido não existia uma grande preocupação com a segurança de rede. Mas, devido ao grande avanço da *Internet*, falhas nos sistemas passaram a ser amplamente divulgadas, crescendo conseqüentemente o número de invasões e ataques aos mesmos.

Assim, o grupo de segurança da IETF iniciou o projeto de um conjunto de padrões voltados à segurança sobre o IP, que foi chamado de *IP Security Protocol* (IPSec) com objetivo de prover segurança no tráfego de dados pela rede com o auxílio da Criptografia, fornecendo proteção tanto ao pacote IP quanto às camadas superiores [Silva, 2003]. A figura 1 apresenta a localização do IPSec no modelo de referência RM-OSI.

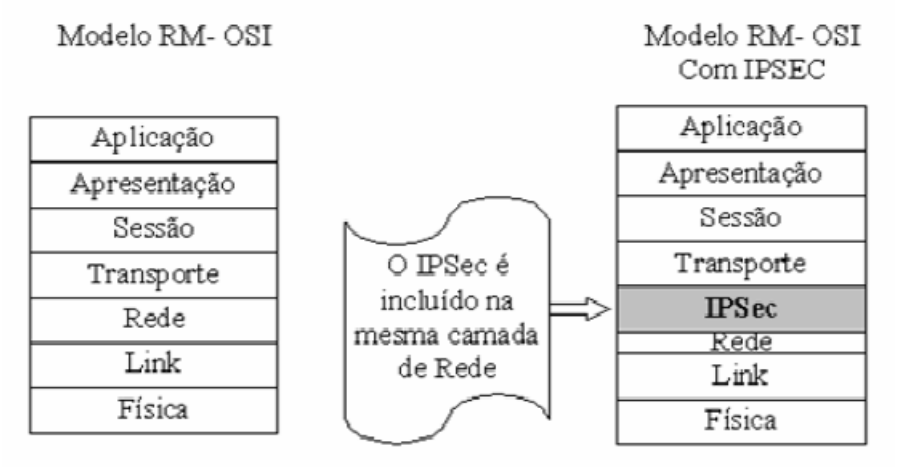


Figura 1 – Localização do ***IPSec*** no modelo RM-OSI

Como pode ser observado na figura, o protocolo IPSec cria uma camada virtual separando a camada de rede em duas camadas, protegendo todo o tráfego da rede e das camadas superiores. Desta forma, a segurança será garantida mesmo que as informações estejam sendo transportadas por meio não seguro, como a *Internet*.

O IPSec integra mecanismos que fornecem ao pacote IP serviços de autenticação, integridade, controle de acesso e confidencialidade na camada de rede. O IPSec foi padronizado para garantir interoperabilidade e mecanismo de criptografia para o IPv6, já que foi projetado paralelamente a este protocolo, mas como a adoção deste novo protocolo está sendo lenta, o IPSec foi adaptado para uso no IPv4 [Silva, 2003].

4.1. Arquitetura do IPSec

Para que sejam alcançados os objetivos do IPSec é necessária à utilização de protocolos de tráfegos seguros, que são: *Authentication Header(AH)* e *Encapsulating Security Payload(ESP)*, e de procedimentos e protocolos de gerência de chaves (IKE). Porém, por ter uma arquitetura aberta, o IPSec possibilita a inclusão de outros algoritmos de autenticação e criptografia [Rotole,2002].

A RFC 2411 disponibiliza o *IP Security Document Roadmap*, que estabelece as diretrizes para a produção de algoritmos e inter relacionamento entre o conjunto de protocolos IPSec, conforme é mostrado na figura 2.

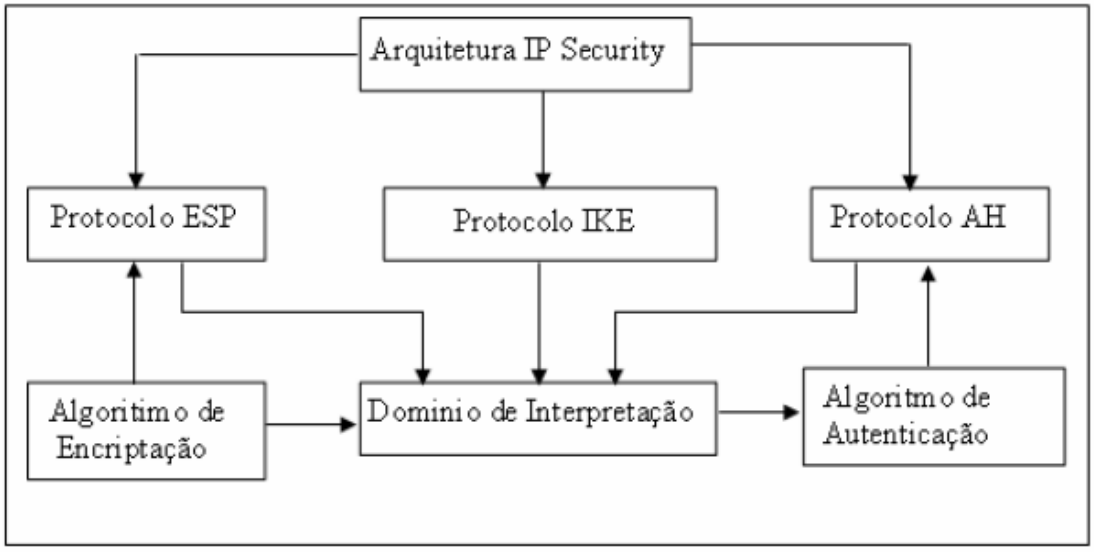


Figura 2 - Arquitetura IPSec, retirado de [Masica, 1998]

A figura 2 demonstra o emprego de três protocolos: O protocolo ESP, o protocolo IKE e o protocolo AH. O protocolo AH (*Authentication Header*) é utilizado para prover os serviços de integridade e autenticação, sendo que não faz cifragem, logo, não garante confidencialidade. O protocolo ESP (*Encapsulating Security Payload*) é utilizado para prover integridade e confidencialidade ao datagrama IP, através da criptografia, garantindo que os dados, além de não sofrerem alteração, sejam visualizados apenas pelo destinatário. O protocolo IKE (*Internet Key Exchange*) é utilizado para a gerência automática das chaves criptográficas, se preocupando em disponibilizar as chaves de forma segura. O IPSec permite que se escolha qual destes protocolos (AH ou ESP) se deseja utilizar para transmitir os dados, ou a utilização simultânea de ambos.

O domínio de interpretação (DOI) funciona como um banco de dados que armazena as informações como: algoritmos obrigatórios e facultativos e identificadores dos protocolos. Estas informações são sempre consultadas durante uma negociação de AS (Associação de Segurança) que é o estabelecimento de um canal seguro.

O IPSec fornece um serviço chamado Associação de Segurança (AS), que é um conceito essencial e consiste em um conjunto de diretivas que permite negociar algoritmos de Criptografia a serem utilizados. Para estabelecer uma comunicação segura tanto o emissor quanto o receptor têm que entrar em um acordo sobre quais mecanismos de segurança utilizarão. A garantia de segurança fica por conta dos protocolos de segurança AH e ESP, sozinhos ou em conjunto. No caso de se usar AH e ESP em conjunto, mais de uma AS deve ser definida [Rotole, 2002].

5. Segurança com o Protocolo IPv6

De acordo com o seu projeto, o IPv6 deve oferecer segurança nativa provida pelo protocolo IPSec, que é uma tentativa de definir uma solução global para o problema de falta de segurança na *Internet* [Santos, 2004]. Porém, além desta segurança, o IPv6 dispõem de outras formas de seguranças, como: sua estrutura de endereços e o *Security Neighbor Discovery*.

GODINHO JR, Luis; SOUSA, Jarbas Pereira Lopes; NUNES, Robert Mady, BOGO, Madianita. Análise da Segurança em Redes Puramente Ipv6. In: VII ENCONTRO DE ESTUDANTES DE INFORMÁTICA DO ESTADO DO TOCANTINS, 2005, Palmas. **Anais...** Palmas: 2005.

A estrutura de endereços, que é formada por 8 (oito) campos com dígitos em hexadecimal separados por (:) dois pontos cada, não possui classes de rede, como em IPv4 que possui rede classe A,B,C, e não possui máscaras de rede, o que dificulta a busca de endereços na rede para tentativa de invasão.

O protocolo *Neighbor Discovery* (NDP) associa o ARP (Protocolo de Resolução de endereços) com os endereços MAC das placas de rede e utiliza mensagens ICMP para a descoberta de roteador (*router discovery*), permitindo autoconfiguração de máquinas IPv6 na rede sem a necessidade de intervenção direta do administrador.

As mensagens do NDP são mensagens ICMPv6, que não usam nenhum tipo de proteção IPSec. E, portanto, o NDP é sujeito a ataques que podem redirecionar o fluxo dos pacotes IP para lugares inconvenientes. Para resolver este problema de segurança e evitar a configuração manual do NDP, o IETF criou o grupo de trabalho, chamado *Securing Neighbor Discovery* (SEND), cujo objetivo é definir o suporte à segurança do NDP, sem a necessidade de acabar com a configuração automática [Santos, 2004].

Uma das principais vantagens que justifica uma migração para o IPv6 é o requisito segurança, que é um problema diário principalmente para as empresas que efetuam ou dispõem a seus clientes transações de valores, como compra e venda pela Web.

6. Avaliação prática da segurança com IPv6 – Windows e Linux

Esse trabalho teve como propósito analisar a segurança que é oferecida, por padrão, pelos sistemas operacionais que implementam protocolo IPv6. Para isso, foram utilizados 3 computadores ligados em rede puramente IPv6, sendo que em dois foi instalado o Windows, 2000 *Professional* e XP *Professional*, e no outro foi instalada a distribuição *Slacware* 10 do Linux.

Para verificar se a segurança nativa está sendo garantida pelos sistemas operacionais que implementam o IPv6, o primeiro teste realizado foi a execução do programa de captura de pacotes Ethereal (*Snnifer*), sem configurar opções de segurança nas máquinas ligadas em rede puramente IPv6. Os dados obtidos pelo programa na troca de informação entre as máquinas (ambas com Windows) são mostrado na figura 3.

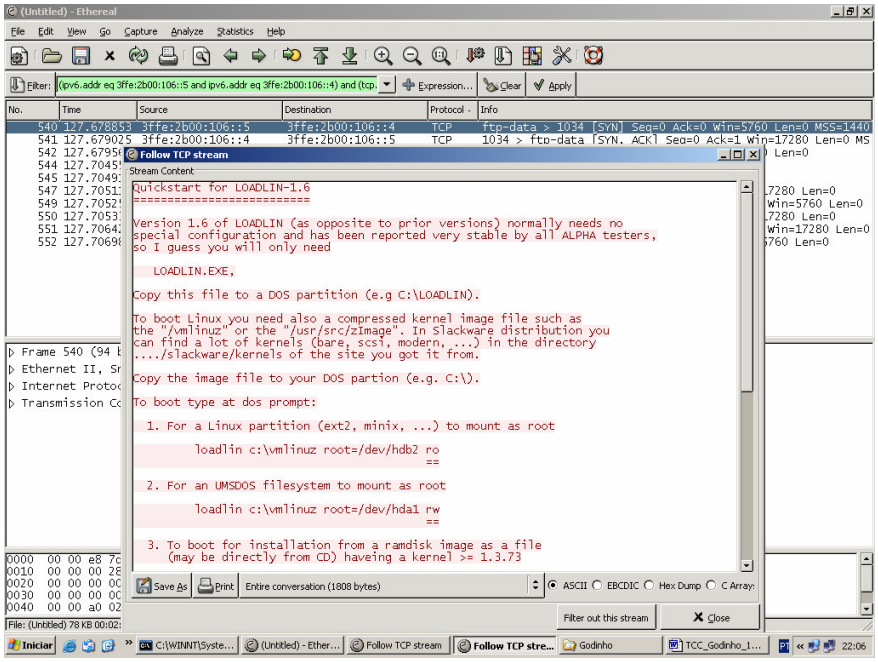
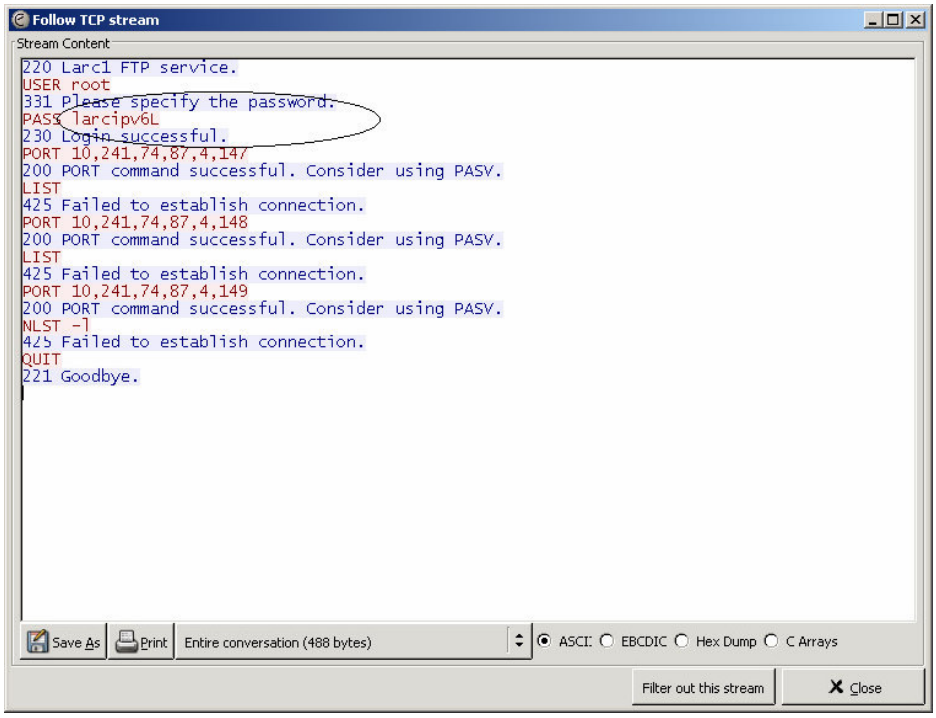


Figura 3 - Tela do Ethereal capturando dados através do endereço IPv6

Como pode ser visto na figura 3, que apresenta o conteúdo do arquivo capturado, foi possível capturar normalmente os arquivos que foram trafegados. Até mesmo os comando digitados durante a conexão FTP foram capturados e puderam ser visualizados, inclusive o usuário e a senha, com pode ser verificado na figura 4.



GODINHO JR, Luis; SOUSA, Jarbas Pereira Lopes; NUNES, Robert Mady, BOGO, Madianita. Análise da Segurança em Redes Puramente Ipv6. In: VII ENCONTRO DE ESTUDANTES DE INFORMÁTICA DO ESTADO DO TOCANTINS, 2005, Palmas. **Anais...** Palmas: 2005.

Figura 4 - Tela do Ethereal com os comandos capturados

Depois dos testes realizados sem a configuração explícita da segurança, o IPSec foi configurado tanto no Windows como no Linux, sendo que neste último foi preciso recompilar o *kernel,* para a realização de novos testes na comunicação, com a transferência de dados com o FTP. Com essa configuração não foi mais possível visualizar os arquivos que estavam sendo transitados, nem os dados da conexão, como usuário e senha. Os novos testes foram realizados entre duas máquinas Windows e entre máquinas Windows e Linux e, nos dois casos, os dados só foram trafegados de forma segura após a configuração do IPSec.

Assim, apesar de teoricamente não ser necessário fazer alterações na configuração padrão para garantir uma segurança básica em redes puramente IPv6, depois da verificação da vulnerabilidade da rede, como pode ser verificado a partir dos resultados apresentados, pôde-se perceber que isso ainda não é implementado na prática, pelo menos pelos sistemas analisados. Talvez pelo fato do IPv6 ainda estar em fase de transição, e não ser efetivamente utilizado, os Sistemas Operacionais ainda estejam deixando a garantia de segurança por conta do usuário, da mesma forma que era no IPv4. Outro motivo que pode ser levado em consideração para que a segurança seja opcional é o desempenho na rede, pois os usuários podem querer oferecer segurança via aplicação, assim como era no IPv4.

7. Conclusões

O projeto do protocolo IPv6 apresenta algumas vantagens sobre o IPv4, sendo que uma das mais importantes é o fato de apresentar segurança mandatária. Essa característica foi instituída pelo IETF com intuito de reduzir a vulnerabilidade no tráfego de dados pela rede pública (*Internet*). Essa segurança nativa é bastante comentada em trabalhos encontrados na *Internet*, porém nenhum desses trabalhos mostra resultados de testes que comprovem esta segurança.

Foi possível perceber, nos Sistemas Operacionais analisados, que a segurança com o IPSec não é "mandatária" conforme é determinado na especificação da IETF, pois antes da configuração do IPSec, mesmo com a utilização de redes puramente IPv6, os dados foram facilmente capturados. Como o IPv6 ainda está em fase de testes, esse pode não ser um problema e sim uma opção dos projetistas dos Sistemas, pois caso a segurança já fosse mandatária neste período transitório IPv4-IPv6 pudesse ocorrer falhas na comunicação entre *hosts*.

O IPv6 apresenta também outras vantagens em relação ao IPv4 no que se refere à segurança, apesar do fato dos Sistemas Operacionais não estarem garantindo a proteção dos dados de forma mandatária, é possível obter mais segurança levando em consideração as características que dizem respeito à estrutura de endereços. O comprimento maior dos endereços e o fato de não apresentar classes de rede e nem mascaramento dificulta a busca de endereços na rede, evitando algumas invasões. Logo, mesmo que a segurança com o IPSec não tenha sido implementada de forma mandatária, é conveniente implantar o IPv6, mesmo que seja como túneis (IPv6 sobre IPv4), pois outros benefícios podem ser obtidos.

GODINHO JR, Luis; SOUSA, Jarbas Pereira Lopes; NUNES, Robert Mady, BOGO, Madianita. Análise da Segurança em Redes Puramente Ipv6. In: VII ENCONTRO DE ESTUDANTES DE INFORMÁTICA DO ESTADO DO TOCANTINS, 2005, Palmas. **Anais...** Palmas: 2005.

8. REFERÊNCIAS BIBLIOGRÁFICAS

[Brocardo, 2001] Trabalho de Pós – Graduação, em Segurança em computação – Instituto Catarinense de Pós-Graduação – ICPG, Indaial, Março de 2001.

[Calado, 2004] Rodrigo Teles Calado - IPv4 para IPv6? Migração ou co-existência? – http://www.ircmania.com.br/artigos.

[Galiano, 1997] Galiano, Herbert Luna; Rochol, Juergen. Segurança em Sistemas de Comunicação Pessoal - Um Estudo Comparativo da Interconexão de Sistemas Heterogêneos. Artigo publicado XV Simpósio Brasileiro de Redes de Computadores. 1997. Disponível em http://labcom.inf.ufrgs.br/artigos/seguranca_em_sistemas.pdf, acesso em Junho de 2004.

[Martins,2000] Dener Lima Fernandes Martins - Redes Privadas Virtuais com IPSec http://www.cic.unb.br/docentes/pedro/trabs/vpn.pdf acessado em maio de 2004.

[Microsoft, 2001] Microsoft corporation; http://www.msnews.microsoft.com, acessado em agosto de 2004.

[Obelheiro,1999] Rafael Rodrigues Obelheiro, Intodução e Histórico do IPv6. http://www.lcmi.ufsc.br/redes/redes99/obelix/IPv6/node1.html acessado em agosto de 2004.

[Puttini, 2003] Puttini, Ricardo Staciarini; Sousa, Rafael Timóteo Jr. Material de Apoio a Disciplina Redes de Computadores: Módulo Criptografia. Disponível em http://www.redes.unb.br/security/, acessado em maio de 2004.

[Rotole,2002] Rotole, Erick Dantas. Arquitetura IP Security - Criptografia e Segurança na Informática, http://www.cic.unb.br/docentes/pedro/trabs/IPsec.rtf acessado em abril de 2004.

[Santos, 2004] Cleymone Ribeiro dos Santos - Integração de IPv6 em um Ambiente Cooperativo Seguro. Dissertação de Mestrado - Instituto de Computação da Universidade Estadual de Campinas. http://www.las.ic.unicamp.br/paulo/teses acessado em outubro de 2004.

[Silva, 2003] Lino Sarlo da Silva – Virtual Private Network (VPN), ED. Novatec.