

**UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO” –  
UNESP**

**LEON KLINKE ANDRE**

**ANÁLISE DE SEGURANÇA DO PROTOCOLO IPV6 UTILIZANDO  
DIFERENTES PLATAFORMAS PARA MÉTODOS DE PEN TEST**

**BAURU**

**2014**

**LEON KLINKE ANDRE**

**ANÁLISE DE SEGURANÇA DO PROTOCOLO IPV6 UTILIZANDO  
DIFERENTES PLATAFORMAS PARA MÉTODOS DE PEN TEST**

Proposta para Trabalho de Conclusão de Curso, pertencente ao curso de Bacharelado em Ciência da Computação e vinculada ao Departamento de Computação da Universidade Estadual Paulista “Júlio de Mesquita Filho” – UNESP.

Orientação: Prof. Dr. Kelton Augusto Pontara da Costa.

**BAURU**

**2014**

**LEON KLINKE ANDRE**

**ANÁLISE DE SEGURANÇA DO PROTOCOLO IPV6 UTILIZANDO  
DIFERENTES PLATAFORMAS PARA MÉTODOS DE PEN TEST**

Trabalho de Conclusão de Curso apresentado ao Departamento de Computação da Universidade Estadual Júlio de Mesquita Filho – UNESP, Câmpus de Bauru, sob orientação do Prof. Dr. Kelton Augusto Pontara da Costa.

**BANCA EXAMINADORA**

Orientador Prof. Dr. Kelton Augusto Pontara da Costa.

Instituição: Universidade Estadual Paulista.

Assinatura: \_\_\_\_\_

Nome: Prof. Dr. Wilson Massashiro Yonezawa

Instituição: Universidade Estadual Paulista.

Assinatura: \_\_\_\_\_

Nome: Prof<sup>a</sup> Dr<sup>a</sup> Humberto Ferasoli Filho.

Instituição: Universidade Estadual Paulista.

Assinatura: \_\_\_\_\_

Universidade Estadual Paulista.

17 de março de 2015.

Dedico esse trabalho à toda minha família, por sempre me apoiar e impulsionar em todos os momentos de minha vida, nunca permitindo que nada faltasse.

## **AGRADECIMENTOS**

Gostaria de demonstrar minha gratidão à minha família por tudo que me proporcionou em todos os momentos da minha vida. Agradeço todas pessoas que estiveram junto à mim nessa jornada da graduação, presente em momentos ruins e outros incríveis. Sou grato também à meus professores que contribuíram muito com seu conhecimento e experiência. Também agradeço a UNESP Bauru pela oportunidade de estar entre todas essas pessoas e me conceder esses quatro anos de aprendizagem.

## **RESUMO**

Atualmente o IPv4 é o protocolo de Internet mais disseminado no mundo, porém seus recursos tem sido exauridos rapidamente com o crescimento exponencial da rede de computadores. O IPv6 é a nova versão do protocolo que comporta esse crescimento e possui um espaço de endereçamento tão grande que seria capaz de conter o crescimento por muitos anos. Porém esse novo protocolo traz consigo novas preocupações acerca de sua segurança, ao passo que esse apresenta uma nova estrutura, novas vulnerabilidades podem ser apresentadas e exploradas.

Já existem trabalhos sobre o IPv6, buscando proporcionar à ele mais segurança e confiabilidade, porém o protocolo ainda é “jovem” e necessita de mais estudos. O presente estudo pretende trazer possíveis vulnerabilidades.

**Palavras-chave:** IPv6, Pen-test, Hacking, Redes, Segurança, Internet.

## **ABSTRACT**

Currently IPv4 is the most widespread Internet protocol in the world, but its resources has been quickly exhausted with the exponential growth of computer network. IPv6 is the Internet protocol's new version, containing this growth and such a large address space, that would be able to contain it for many years. But this new protocol brings new concerns about its safety, while this presents a new structure, also new vulnerabilities can be presented and exploited. There are works on IPv6, seeking to provide it more safety and reliability, but the protocol is still "young" and needs further studies. This research aims to bring to light some of their vulnerabilities.

**Keywords:** IPv6, Pen-test, Hacking, Network, Security, Internet.

## **LISTA DE QUADROS**

Quadro 1 - Ferramentas utilizadas .....	40
Quadro 2 - Resultados .....	54



## **LISTA DE ABREVIATURAS E SIGLAS**

CPU	Central Processing Unit
DDOS	Distributed Denial Of Service
DOS	Denial Of Service
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
ICMPV6	Internet Control Message Protocol Version 6
IP	Internet Protocol
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
MITM	Man In The Middle
RFC	Request for Comments
THC	The Hacker Choice
UDP	User Datagram Protocol
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network

## LISTA DE FIGURAS

Figura 2.1.1 - Cabeçalho IPv4.....	19
Figura 2.1.2 - Esgotamento do IPv4.....	20
Figura 2.1.3 - Cabeçalho IPv6.....	21
Figura 2.1.4 - Implantação do IPv6.....	21
Figura 2.1.5 - Comunicação em rede.....	22
Figura 2.1.6 - Firewall de filtragem de pacotes.....	23
Figura 2.1.7 - Gateway de aplicação.....	25
Figura 2.1.8 - IDS.....	26
Figura 2.1.9 - Criptografia de chave simétrica.....	28
Figura 2.2.1 - Criptografia de chave assimétrica.....	29
Figura 2.2.2 - Spoofing.....	33
Figura 2.2.3 - Modo Promíscuo.....	34
Figura 2.2.4 - Sniffing.....	35
Figura 2.2.5 - MitM.....	36
Figura 2.2.6 - DoS.....	37
Figura 2.2.7 - DDoS.....	38
Figura 3.1.1 - Sistemas Operacionais mais usados.....	41
Figura 3.1.2 - Laboratório para testes.....	42
Figura 3.1.3 - Windows XP antes do ataque.....	43
Figura 3.1.4 - Windows 7 antes do ataque.....	44
Figura 3.1.5 - Ubuntu antes do ataque.....	44
Figura 3.1.6 - Kali flood_router.....	45
Figura 3.1.7 - Windows 7 durante ataque flood_router.....	46
Figura 3.1.8 - Windows XP durante ataque flood_router.....	46
Figura 3.1.9 - Ubuntu durante ataque flood_router.....	47
Figura 3.2.1 - Kali Linux durante ataque DoS.....	48
Figura 3.2.2 - Windows 7 durante ataque DoS.....	49
Figura 3.2.3 - Ubuntu durante ataque DoS.....	49
Figura 3.2.4 - Windows XP durante ataque DOS.....	50
Figura 3.2.5 - Kali Linux alive6.....	51
Figura 3.2.6 - Windows 7 Ping -6.....	51

Figura 3.2.7 - Kali Linux parasite6.....	52
Figura 3.2.8 - Kali Linux Wireshark.....	53

## SUMÁRIO

<b>1 INTRODUÇÃO .....</b>	<b>13</b>
1.1 OBJETIVO GERAL.....	14
1.2 OBJETIVO ESPECÍFICO.....	14
1.3 JUSTIFICATIVA.....	14
<b>2 REFERENCIAS BIBLIOGRÁFICA.....</b>	<b>15</b>
2.1 FUNDAMENTOS DE REDE .....	15
2.1.1 O QUE É A INTERNET .....	15
2.1.2 MODELO OSI .....	16
2.1.3 SOCKETS .....	18
2.2 FUNDAMENTOS DO IP .....	18
2.2.1 IPV4 .....	18
2.2.2 IPV6 .....	20
2.2.3 TRANSIÇÃO IPV4-IPV6 .....	22
2.3 SEGURANÇA EM REDES DE COMPUTADORES .....	22
2.4 FIREWALL .....	23
2.4.1 FIREWALL DE FILTRAGEM DE PACOTES .....	24
2.4.2 GATEWAYS DE CAMADA DE APLICAÇÃO .....	25
2.5 IDS (INTRUSION DETECTION SYSTEM) .....	26
2.6 CRIPTOGRAFIA .....	27
2.6.1 CRIPTOGRAFIA SIMÉTRICA .....	27
2.6.2 CRIPTOGRAFIA ASSIMÉTRICA.....	28
2.7 FUNDAMENTOS DO HACKING.....	29
2.8 TESTE DE PENETRAÇÃO (PENTEST) .....	30
2.9 ATAQUES.....	31
2.9.1 ATAQUE DIRETO .....	31
2.9.2 ATAQUE INDIRETO.....	31
2.9.3 COLETA DE INFORMAÇÃO .....	32
2.9.4 SPOOFING .....	32
2.9.5 SNIFFING .....	33
2.9.6 MITM - MAN-IN-THE-MIDDLE .....	35
2.9.7 DOS - DENIAL OF SERVICE .....	36
2.9.8 DDOS - DISTRIBUTED DENIAL OF SERVICE .....	37
2.10 SEGURANÇA NO IPV6 .....	38

2.10.1 THC IPV6 TOOLKIT .....	39
<b>3 METODOLOGIA.....</b>	<b>40</b>
<b>4 TESTES DE ATAQUES .....</b>	<b>43</b>
4.1 <i>FLOOD</i> .....	43
4.2 DOS.....	47
4.3 MITM.....	50
<b>5 RESULTADOS.....</b>	<b>54</b>
<b>6 CONCLUSÕES.....</b>	<b>55</b>
<b>REFERÊNCIAS .....</b>	<b>56</b>

## CAPÍTULO 1 INTRODUÇÃO

A internet hoje é uma ferramenta quase indispensável para as mais diversas atividades do nosso dia-a-dia, estando presente em nosso trabalho, em nossa casa e em nossos momentos de lazer. (FLORENTINO, 2012, p.3).

"O protocolo de internet é projetado para o uso em de sistemas interconectados por troca de pacotes. O protocolo possibilita a transmissão de blocos de dados chamados de datagramas, da fonte para os destinos, onde ambos, fonte e destinos, são 'hosts' identificados por endereços de tamanhos fixos" (University of Southern California, 1981). "Existem hoje dois tipos de protocolos publicamente disponíveis, chamados Protocolo de Internet versão 4 (IPv4) e o Protocolo de Internet versão 6 (IPv6). (Pilihanto, 2011, p.2).

McCumber (1991) afirma que confidencialidade, autenticação, integridade e não-repudição de mensagem vem sendo considerados componentes fundamentais da comunicação segura há bastante tempo. "Disponibilidade e controle de acesso são extensões mais recentes da noção de comunicações seguras". (Maconachy, 2001, p.345). Para Kurose e Ross essas comunicações seguras são motivadas pelas preocupações muito reais com a segurança da infra-estrutura de rede contra um potencial ataque violento dos 'bandidos'. Um dos modos mais seguros para garantir que pessoas mal intencionadas não possam causar danos é assegurar, antes de mais nada, que seus pacotes não entrem na rede. Um firewall é um dispositivo situado entre a rede a ser protegida e o resto do mundo. Ele controla o acesso de e para a rede regulando quais pacotes podem passar para dentro e para fora dela. (2006, p. 514).

Todas as melhores práticas que temos com relação ao *hardening* (fortalecimento) dos mecanismos de segurança, à política de segurança, as ferramentas usadas e mesmo ao treinamento de profissionais da área são baseadas em IPv4. Incidentes de seguranças envolvendo IPv6 e o uso de ferramentas criadas para explorar vulnerabilidades do novo protocolo da Internet são conhecidos desde o início dos anos 2000. Muitas destas vulnerabilidades ainda não foram totalmente corrigidas e destas vulnerabilidades que ainda não foram totalmente corrigidas, serão com o tempo e a adoção massiva do protocolo. Com um universo maior de profissionais utilizando o IPv6, as vulnerabilidades serão publicadas e corrigidas em uma velocidade cada vez maior. (Florentino, 2012, p.79).

O presente estudo propõe explorar vulnerabilidades do tipo *Flood*, *Dos* e *MitM* buscando proporcionar segurança para o uso do IPv6.

## 1.1 OBJETIVO GERAL

Analisar possíveis vulnerabilidades utilizando o protocolo IPv6, mais precisamente dos tipos *Flood*, *Dos* e *MitM*, avaliando o comportamento de sistemas operacionais, visando identificar métodos para solucionar as referidas vulnerabilidades caso sejam identificadas.

## 1.2 OBJETIVO ESPECÍFICO

- Entender as estruturas presentes no protocolo IPv6, desde cabeçalhos, formas de comunicação e tunelamento, procurando por vulnerabilidades dos tipos *Flood*, *Dos* e *MitM* presentes no protocolo e se possível propor soluções.
- Elaborar uma pesquisa sobre vulnerabilidades, proporcionando uma documentação recente que poderá auxiliar em outras pesquisas.

## 1.3 JUSTIFICATIVA

Não se pode dizer com certeza que as novas tecnologias são as mais seguras, o protocolo IPv6 em si ainda é pouco conhecido e disseminado para se dizer seguro, sua implementação é muito tímida neste últimos 13 anos. Explorar suas falhas e desenvolver pesquisas de segurança é vital para uma melhor adequação de sua tecnologia, bem como embasar um material de apoio para empresas que implementam o IPv6.

## **CAPÍTULO 2 REFERENCIAS BIBLIOGRÁFICA**

A seguir será descrito conceitos sobre assuntos referidos à segurança em redes e o protocolo IPv6, assunto principal a ser abordado nesse trabalho.

### **2.1 FUNDAMENTOS DE REDE**

Para Erickson (2008, p.195) A comunicação sempre teve uma grande importância no desenvolvimento da raça humana.

Programas se tornam muito mais poderosos quando são capazes de trocar informações com outros via rede. Muito do que esta em nosso cotidiano como emails, Web, possuem algum protocolo e utilizam a ideologia da rede para se comunicar.

Para compreender melhor os fundamentos das redes de computadores, é importante entender o que é a internet.

#### **2.1.1 O QUE É A INTERNET**

Kurose e Ross (2006, p.3) definem a Internet da seguinte maneira: "a Internet pública é uma rede de computadores mundial, isto é, uma rede que interconecta milhões de equipamentos de computação em todo o mundo. Não faz muito tempo, esses equipamentos eram primordialmente PCs tradicionais de mesa, estações de trabalho com sistema Unix e os chamados servidores que armazenam e transmitem informações, como páginas Web e mensagens de e-mail. [...] Realmente, o termo *rede de computadores* está começando a soar um tanto desatualizado, dados os muitos equipamentos não tradicionais que estão sendo ligados à Internet. No jargão da Internet, todos esses equipamentos são denominados *hospedeiros* ou *sistemas finais*. Em janeiro de 2003, havia mais de 233 milhões de sistemas finais usando a Internet, e esse número continua a crescer rapidamente".

A comunicação entre os dispositivos de uma rede necessita de uma "linguagem" que todos possam compreender. O modelo OSI é uma forma muito utilizada como referência de comunicação hoje em dia.



### **2.1.2 MODELO OSI**

"Quando dois computadores conversam entre si, eles precisam conversar a mesma língua. A estrutura dessa comunicação é descrita em camadas pelo modelo OSI. Esse modelo prove padrões que permitem o hardware, assim como os roteadores e firewalls, focarem em um aspecto de comunicação em particular que aplicam uns e ignoram outros [...] Dessa maneira, roteadores e firewalls podem focar em passar informações para os níveis mais profundos ignorando o que acontece mais acima usados por aplicações" Erickson (2008, p.196).

As sete camadas descritas pelo modelo OSI são:

- Camada física
- Camada de enlace
- Camada de rede
- Camada de transporte
- Camada de sessão
- Camada de apresentação
- Camada de aplicação

Nesse estudo é abordado algumas das principais camadas.

#### **(i) CAMADA DE APLICAÇÃO**

De acordo com Kurose e Ross (2006, p.37) "a camada de aplicação é onde residem aplicações de rede e seus protocolos". É nessa camada que se encontram protocolos como o HTTP (disponibiliza requisições e transferência de documentos via web) e o FTP (disponibiliza transferência de arquivo entre dois hospedeiros) por exemplo.

#### **(ii) CAMADA DE TRANSPORTE**

Ainda Kurose e Ross (2006, p.37) descrevem a camada de transporte como uma camada que realiza o transporte, do lado da aplicação para o servidor desta. Os dois principais protocolos presentes nessa camada são:

- TCP:

Garante a entrega das mensagens da camada de aplicação ao destino e controle de fluxo (controla a velocidade como que essa mensagem é transmitida).

- UDP:

É um serviço mais indicado para grandes volumes de dados, não garante necessariamente que todos os pacotes serão entregues, mas os transfere de maneira rápida.

### **(iii) CAMADA DE REDE**

Para Kurose e Ross (2006, p.42) a camada de rede é responsável pela movimentação, de uma máquina para a outra, de pacotes em forma de *datagramas*.

"Exatamente como você passaria ao serviço de correios uma carta com o endereço de destinatário. A camada de rede então provê o serviço de entrega do segmento à camada de transporte na máquina destinatária". Kurose e Ross (2006, p.37).

### **(iv) CAMADA DE ENLACE**

Segundo Erikson (2008, p.218) a camada de enlace é como se fosse um serviço de correio global, onde os datagramas são enviados de roteador à roteador afim de chegar em seu destino. Kurose e Ross definem esses pacotes na camada de enlace como *quadros*.

### **(v) CAMADA FÍSICA**

Kurose e Ross (2006, p.45) definem essa camada como a mais baixa de todas. Enquanto a camada de enlace é encarregada de movimentar os quadros de um elemento de rede (roteadores por exemplo) para o outro a camada física movimenta os *bits individuais* que estão dentro do quadro de um nó para o seguinte.

O presente estudo faz uso de rotinas que constantemente enviam e recebem dados pela rede, para um maior entendimento de como elas funcionam, é muito importante o entendimento dos *Sockets*.

### 2.1.3 SOCKETS

Para Erickson (2008, p.198) um *socket* é uma maneira padrão de comunicação com a rede pelo sistema operacional, assim como soquete em um quadro de distribuição. Porém esses sockets não existem de fato, são apenas uma abstração criada por programadores. Para estes os sockets são uma porta de comunicação com a rede, onde podemos enviar ou receber dados. Esses dados são transmitidos na camada de sessão, acima das mais profundas. Existem muitos tipos de sockets, mas os mais comuns são os *stream sockets* e *datagram sockets*.

- Stream sockets: utilizam o protocolo TCP.
- datagram sockets: utilizam o protocolo UDP.

Em linguagens de programação como C, as funções de sockets são bem definidas, algumas delas são:

- socket ( int domain, int type, int protocol).
- connect( int fd, struct sockaddr \*remote\_host, socklen\_t addr\_length).
- bind ( int fd, struct sockaddr \*local\_addr, socklen\_t addr\_length).
- listen ( int fd, int backlog\_queue\_size).
- accept ( int fd, struct sockaddr \*remote\_host, socklen\_t \*addr\_length).
- send ( int fd, void \*buffer, size\_t n, int flags).
- recv ( int fd, void \*buffer, size\_t n, int flags).

## 2.2 FUNDAMENTOS DO IP

Quando se deseja enviar uma correspondência para alguém é necessário o endereço do remetente (único para cada um) e uma companhia de transporte para que entregue o pedido.

Na internet é observada a mesma ideia. O IP (Internet Protocol) é o endereço para que a rede mundial possa encontrar um dispositivo, seja para responder um pedido de uma página web, cadastro. ou mesmo que infelizmente, expor seus dados.

### 2.2.1 IPV4

Quando se envia correspondências é necessário indicar para quem se quer enviar, o endereço do remetente caso o dispositivo não seja encontrado, data, etc. Com os pacotes que navegam a internet acontece a mesma coisa, essa informações se encontram em uma estrutura

chamada cabeçalho, cada datagrama (pacote) possui o seu, nessa estrutura pode-se visualizar claramente a diferença entre as versões do protocolo IP.

Como apontado por Florentino (2012, p.23) o IPv4 (Internet Protocol version 4) é a versão do protocolo IP mais disseminada no mundo hoje, seu endereçamento possui 32 bits e mais de 4 bilhões de endereços possíveis, o que na época que foi implantado (1983) parecia um número mais que suficiente para comportar toda a rede de computadores.

O cabeçalho do IPv4 é composto da seguinte forma, conforme descrito na figura 2.1.1:

Figura 2.1.1 - Cabeçalho IPv4

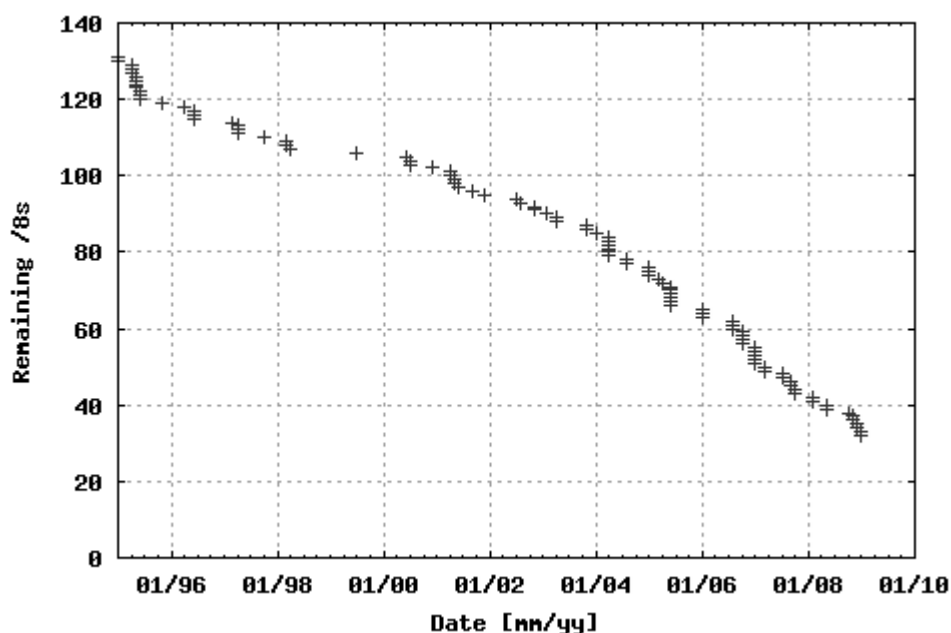
Versão	Comprimento do cabeçalho	Tipo de serviço	Comprimento do datagrama (bytes)	
Identificador de 16 bits		Flags	Deslocamento de fragmentação (13 bits)	
Tempo de vida	Protocolo da camada superior		Soma de verificação do cabeçalho	
Endereço IP de 32 bits da fonte				
Endereço IP de 32 bits do destino				
Opções (se houver)				
Dados				

Fonte: Kurose e Ross (2006, p.256) (adaptado pelo autor)

Florentino também afirma que hoje o esgotamento do IPv4 é real, a primeira região a ter seus endereços IPv4 exauridos será a Ásia (controlada pela APNIC ou Asia-Pacific Network Information Center).

O esgotamento do protocolo foi maior do que o esperado pelos idealizadores do IPv4, como representado na figura 2.1.2:

Figura 2.1.2 - Esgotamento do IPv4



Disponível em: <http://upload.wikimedia.org/wikipedia/commons/9/97/Ipv4Exaustao.png>

Para Pilihanto (2012, p.4) o esgotamento do Protocolo se deu pela explosão de novos usuários por todo o mundo, de forma que em alguns anos não poderemos mais adquirir endereços IPv4, sendo necessário a disseminação de um novo protocolo.

### 2.2.2 IPV6

Com o rápido esgotamento do IPv4 foi necessária a criação de um novo protocolo que comportasse o grande volume de endereços na rede mundial de computadores. Segundo Kurose e Ross (2006, p.270), os projetistas do IPv6 também usaram da oportunidade de criar um novo protocolo para aprimorar o anterior, adotando algumas mudanças, entre elas:

- Maior capacidade de endereçamento: O IPv6 possui um endereço de 128 bits, o que remete a 340 undecilhões de endereços possíveis.
- Cabeçalho fixado em 40 bytes: Eliminou alguns campos do cabeçalho IPv4 e fixou o tamanho para garantir um processamento mais veloz.
- Rotulação de fluxo e prioridade: O IPv6 permite rotular os pacotes em suas rotas, garantindo um serviço mais rápido para alguns usuário que necessitam de prioridade.

O cabeçalho do IPv6 é mostrado na figura 2.1.3:

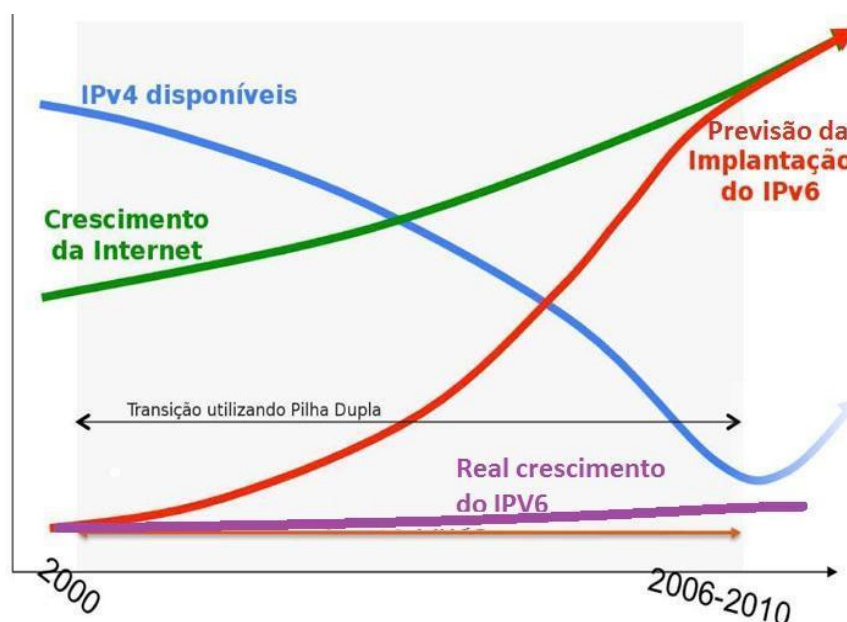
Figura 2.1.3 - Cabeçalho IPv6

Versão	Classe de tráfego	Rótulo de fluxo	
Comprimento da carga útil		Próximo cabeçalho (Hdr)	Limite de saltos
Endereço da fonte (128 bits)			
Endereço do destino (128 bits)			
Dados			

Fonte: Pilihanto (2011, p.3) (adaptado pelo autor)

Mesmo com o crescente esgotamento do IPv4, o IPv6 ainda possui uma implementação muito tímida nesses últimos anos. A figura 2.1.4 expõe a expectativa de adoção do protocolo e a realidade de sua implantação.

Figura 2.1.4 - Implantação do IPv6



Fonte: [moodle.inatel.br/moodle/livrodigital/ipv6/images/modulo/002.jpg](http://moodle.inatel.br/moodle/livrodigital/ipv6/images/modulo/002.jpg) (adaptado pelo autor)

Segundo Florentino (2012, p.22), a lenta aderência do IPv6 no mercado mundial se dá ao fato de que essa transição não traz aos investidores nenhum benefício à curto prazo, além de ter um custo considerável. Más é vital para os provedores de internet se preocuparem com

a implantação do protocolo, pois em breve não haverá mais endereços IPv4 disponíveis, de forma que a migração se torne cada vez mais custosa e dificulte a competitividade com seus rivais.

### 2.2.3 TRANSIÇÃO IPV4-IPV6

A nova tecnologia não é sinônimo de mais segura, de forma que o IPv6 assim como o IPv4 possui suas vulnerabilidades.

Não existe uma data pré-determinada para a implantação definitiva do IPv6, de forma que é necessária a coexistência dos dois protocolos. Para que os esses sejam reconhecidos na mesma rede foram desenvolvidas algumas técnicas. Por exemplo, o tunelamento (*túneis 6to4*, *ISATAP* e *Teredo*), "os túneis *6to4* precisam de *relays* públicos que estão sujeitos a ataques de negação de serviço (*DoS* e *DDoS*) e a técnica do *spoofing* (técnica de subversão de sistemas que consiste em mascarar *spoof* pacotes IP utilizando endereços de remetente falsificados. As vulnerabilidades do IPv4 continuam presentes e agora estão convivendo com as novas vulnerabilidades do IPv6" (Florentino, 2012, p.80).

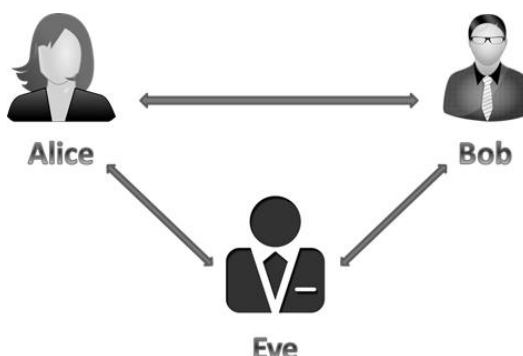
São pertinentes os estudos acerca da segurança de ambos os protocolos, uma vez que estão ligados até hoje.

## 2.3 SEGURANÇA EM REDES DE COMPUTADORES

Segundo Kurose e Ross (2006, p.512). Podemos definir segurança em redes de computadores utilizando um exemplo bem simples.

Considerando um cenário com três componentes, Alice Bob e Eve, onde Alice tenta se comunicar com Bob mas Eve é um atacante que procura interceptar a comunicação entre os dois, como ilustra a figura 2.1.5 :

Figura 2.1.5 - Comunicação em rede



Fonte: [resources.infosecinstitute.com/wp-content/uploads/061713\\_1855\\_NearFieldCo8.png](https://resources.infosecinstitute.com/wp-content/uploads/061713_1855_NearFieldCo8.png)

É importante salientar que Alice e Bob poderiam ser também roteadores que querem trocar tabelas de roteamento com segurança, um cliente e um servidor que querem estabelecer uma conexão segura ou duas aplicações de e-mail.

Kurose e Ross (2006, p.514) não definem comunicação segura apenas como proteção, segundo eles na prática a segurança não envolve apenas proteção, mas também detecção de falhas em comunicações seguras e ataques à infra-estrutura e reação a esses ataques. "em muitos casos, um administrador pode implementar mecanismos especiais de proteção para reagir a ataques". De forma que a segurança é conseguida através de uma preocupação continua com a proteção, detecção e reação.

Uma das principais ferramentas quando se fala em segurança de computadores é o firewall.

## 2.4 FIREWALL

De acordo com Kurose e Ross (2006, p.541) firewall é uma solução composta por hardware e software afim de filtrar o tráfego de rede protegendo a rede interna, permitindo alguns pacotes e restringindo outros.

De maneira similar Nestler et al. (2011, p.186) afirma que "um firewall é um dispositivo que bloqueia tráfego da internet baseado em regras".

Um dos desafios de um firewall eficiente se encontra em conseguir uma configuração não muito leniente, mas também não muito intransigente.

Existem dois tipo de Firewall: *firewall de filtragem de pacotes* e *gateways de camada de aplicação*.

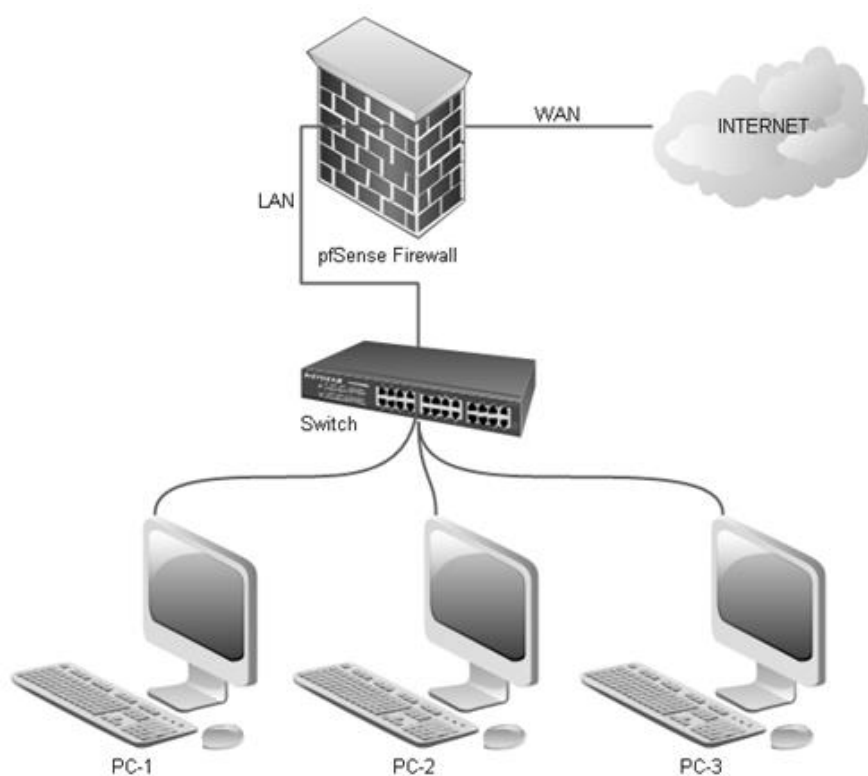


### 2.4.1 FIREWALL DE FILTRAGEM DE PACOTES

Como apontado por Kurose e Ross (2006, p.543) em geral as organizações possuem um roteador na ponta de suas redes, de forma que todo trafego que entra e sai passa por ele, é nesse ponto que se concentra a filtragem de pacotes. A filtragem utiliza cabeçalhos de pacotes (datagramas) e aplica suas regras para determinar se o pacotes será aceito ou não.

A imagem 2.1.6 ilustra a disposição de um firewall de filtragem de pacotes.

Figura 2.1.6 - Firewall de filtragem de pacotes



Fonte: [maxisys.com.br/wp-content/uploads/2014/09/diagramfirewall-maxisys.com\\_.br\\_.png](http://maxisys.com.br/wp-content/uploads/2014/09/diagramfirewall-maxisys.com_.br_.png)

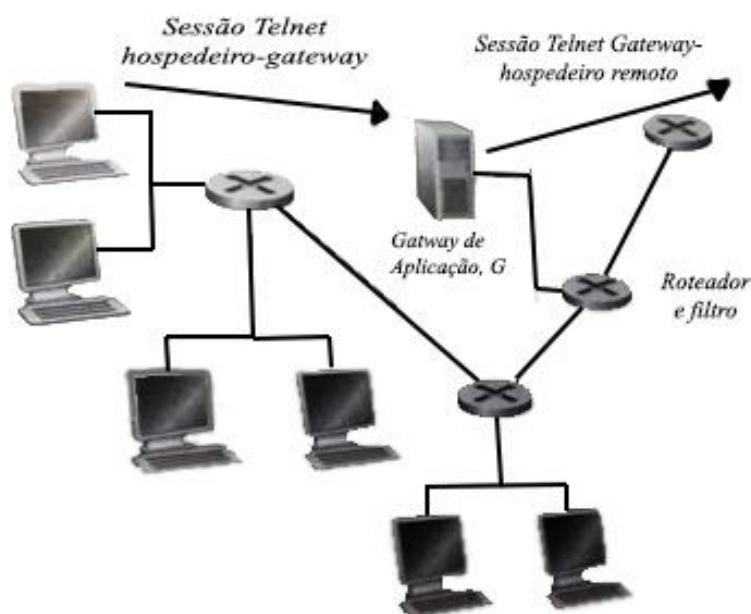
## 2.4.2 GATEWAYS DE CAMADA DE APLICAÇÃO

De acordo com Kurose e Ross (2006, p.544) o firewall de filtragem de pacotes faz uma filtragem grosseira de cabeçalhos, para garantirmos uma maior sofisticação nessa etapa os firewall devem combiná-los com os gateways de aplicação, que fazem mais do que examinar cabeçalhos IP/TCP/UDP.

Kurose e Ross (2006, p.545) definem gateway de aplicação como “é um servidor específico de aplicação através do qual todos os dados da aplicação (que entram e saem) devem passar. Vários gateways de aplicação podem executar o mesmo hospedeiro, mas cada gateway é um servidor separado, com seus próprios processo”.

A imagem 2.1.7 mostra o esquema de um gateway de aplicação.

Figura 2.1.7 - Gateway de aplicação



Fonte: Redes de computadores e a Internet (2006)

Outro componente indispensável para assegurar a segurança de um sistema é o IDS.

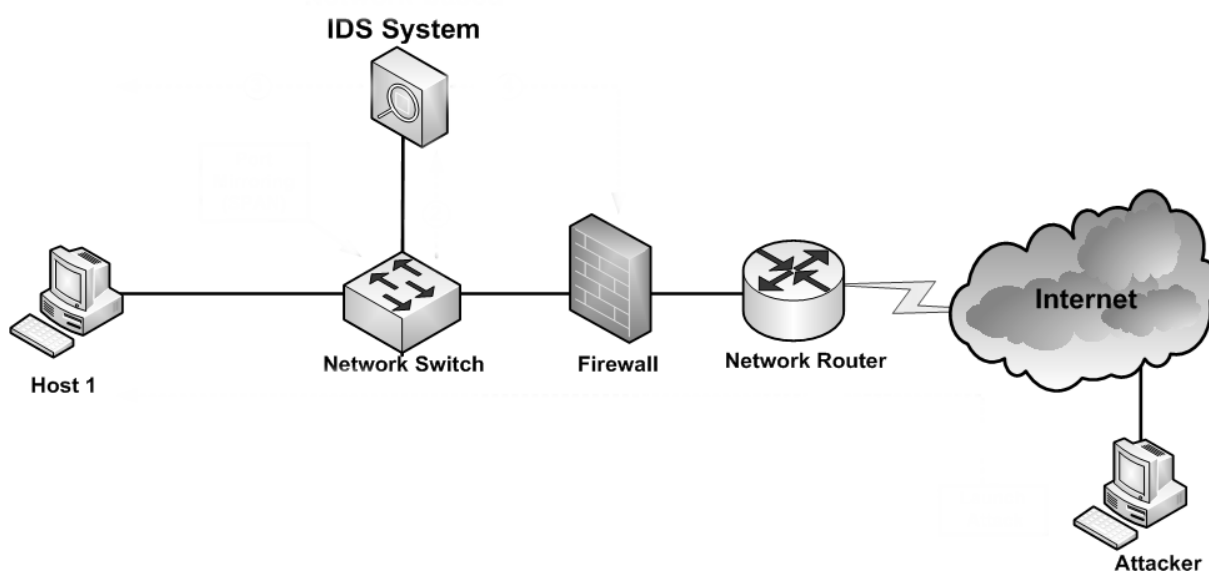
## 2.5 IDS (INTRUSION DETECTION SYSTEM)

Segundo Scanfone e Mell (2007, p.13) existem vários tipo de sistemas de detecção de intrusão, mas todos possuem o mesmo foco, identificar possíveis ameaças. Existem IDSs que emitem alertas quando algum atacante comprometeu o sistema explorando alguma de suas vulnerabilidades, possibilitando que os administradores possam utilizar contramedidas à tempo. Mas a grande maioria dos IDSs são configurados juntamente com os firewalls de forma que não apenas avisam sobre uma ameaça, mas também evitam que está logre sucesso, utilizando de regras que monitoram os dados, bloqueando os que são suspeitos.

Ainda Scanfone e Mell(2007, p.13) afirma que muitos IDSs identificam atividades reincidentes, que indicam possíveis ameaças como *port-scans*, *malwares*, etc.

A figura 2.1.8 mostra a disposição de um IDS na rede.

Figura 2.1.8 - IDS



Fonte: [s10.postimg.org/4467u4oc9/mod8\\_fig1.png](http://s10.postimg.org/4467u4oc9/mod8_fig1.png) (alterado pelo autor)

Outro importante componente quando se refere à segurança de informação é a criptografia.

## **2.6 CRIPTOGRAFIA**

"Criptologia é definida como o estudo da criptografia o criptoanálise. Criptografia é simplesmente o processo de comunicação segura através do uso de cifras e a criptoanálise é o processo de decifrar essas cifras" Erickson (2008, p.393).

Segundo Kurose e Ross (2006, p.515) a criptografia é um mecanismo de proteção de mensagens muito antigo que data desde a época do período Romano. Para Erickson (2008, p.394) historicamente, a criptologia teve um interesse particular em tempos de guerra, onde a comunicação entre as tropas eram ao máximo codificadas para o caso de serem interceptadas, como também a tentativa de "quebra" de cifras inimigas para infiltrar na comunicação inimiga.

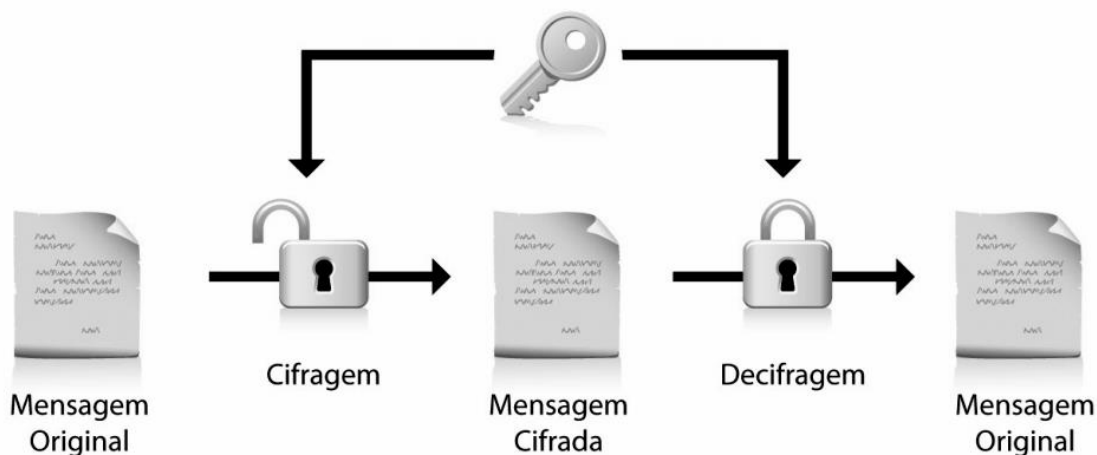
Erickson também afirma que hoje criptografia é cada vez mais presente na rotina do usuário comum, protegendo comunicações e transações pela internet.

Segundo Oliveira (2012, p.2) se apresentam dois tipos básicos de criptografia: a simétrica (chave privada), e a assimétrica (chave pública).

### **2.6.1 CRIPTOGRAFIA SIMÉTRICA**

De acordo com Erickson (2008, p.398) a criptografia simétrica utiliza de um criptosistema que usa a mesma chave para encriptar e descriptar mensagens, esses processo é geralmente mais rápido do que os de chaves assimétricas, mas a distribuição dessas chaves pode ser difícil. A proposta da criptografia simétrica é exposta na figura 2.1.9.

Figura 2.1.9 - Criptografia de chave simétrica



Fonte: [biblioo.info/wp-content/uploads/2012/11/Certifica%C3%A7ao-digital-1-1024x460.png](http://biblioo.info/wp-content/uploads/2012/11/Certifica%C3%A7ao-digital-1-1024x460.png)

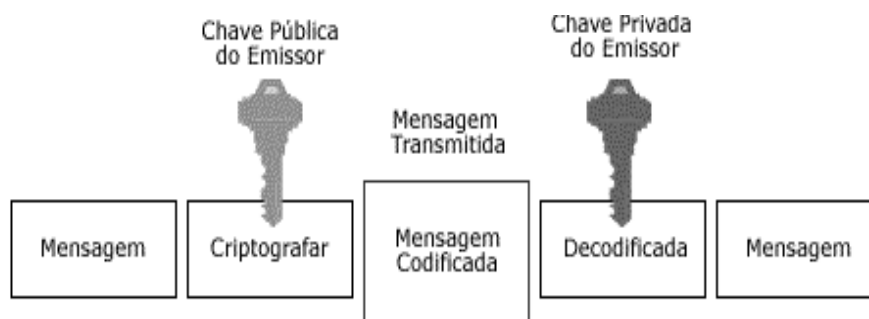
Para Oliveira (2012, p.3) a criptografia simétrica não garante os princípios de autenticidade e não-repudição, e seus principais algoritmos são:

- AES: Advanced Encryption Standard
- DES: Data Encryption Standard
- 3DES: Uma variação do algoritmo DES utilizando três ciframentos sucessivos
- IDEA: International Data Encryption Algorithm
- Blowfish
- Twofish
- RC2
- CAST

## 2.6.2 CRIPTOGRAFIA ASSIMÉTRICA

A criptografia assimétrica usa de duas chaves para a cifragem, uma chave pública e uma privada. De forma que uma mensagem é cifrada com um par, sendo a chave privada quem cifra a mensagem e a correspondente privada quem decifra no destino, o que remove o problema de distribuição da chave, porém tende a tornar o processo um pouco mais lento. Erickson (2008, p.400). O funcionamento da criptografia assimétrica é visto na figura 2.2.1.

Figura 2.2.1 - Criptografia de chave assimétrica



Fonte: [conteudo.imasters.com.br/4802/figura2.gif](http://conteudo.imasters.com.br/4802/figura2.gif)

Segundo Oliveira (2012, p.4) os principais algoritmos de chave pública são:

- RSA
- Elgamal
- Diffie-Hellman
- Curvas Elípticas

## 2.7 FUNDAMENTOS DO HACKING

Ao contrário do que é comumente dito, a prática do Hack não se limita à maneiras ilegais do uso da tecnologia.

Para Erickson (2008, p.2) os verdadeiros Hackers são pessoas que possuem profundo conhecimento computacional, são capazes de entender todo o funcionamento de um sistema, sendo capazes de manipulá-lo de diversas formas. É uma confusão comum dizer que Hacker são pessoas mal intencionadas, que querem roubar nossos dados e invadir sistemas causando problemas.

A definição correta de um infrator da lei por meios digitais é "Cracker", responsável por quebra de sigilo, invasão de sistemas, roubo de dados, terrorismo digital, etc.

Erickson (2008, p.2) também afirma que em geral os Hacker possuem muito mais qualidade técnica e intelectual sobre os sistemas do que os Crackers, estes não possuem total conhecimento do que fazem, ou do que estão lidando, apenas encontram meios de burlar a segurança de sistemas.

Este estudo utilizará técnicas de Hack para expor vulnerabilidades do protocolo IPv6. Não com o intuito de tirar vantagem dessas, mas sim de proporcionar um documento que as liste de forma clara, para que profissionais de segurança possam solucioná-las ou precavê-las.

## 2.8 TESTE DE PENETRAÇÃO (PENTEST)

*Pentest* ou teste de penetração é um método usado para encontrar possíveis falhas de segurança em um sistema computacional.

Para Kennedy et al. (2011, p.xxii) companhias do mundo todo investem milhões de dólares para manter suas informações seguras. Sendo o *Pentest* um dos métodos mais efetivos para prevenir e identificar pontos fracos na segurança dos sistemas.

Hoje, é muito comum que empresas contratem profissionais para realizar os testes em seus sistemas, cabendo a estes a tarefa de pensar como um *Cracker*, simulando um ambiente real de invasão. Seu objetivo é identificar e listar todas as possíveis "brechas" encontradas no sistema.

Kennedy et al. (2011) também listam as fases do *Pentest* para que se possa simular as tentativas de ataque:

- *Pre-engagement Interactions:*  
Define o escopo das tentativas de invasão e as regras com o cliente.
- *Intelligence Gathering:*  
Levanta o maior número de informação possível sobre o alvo. Através de mídias sociais, registros até mesmo imagens de satélite.
- *Threat Modeling:*  
Usa as informações adquiridas na fase anterior para traçar estratégias acerca dos ataques, tenta estabelecer as melhores formas de invadir o alvo baseado no que se parece ser mais vulnerável, este é um tipo de fase usada neste trabalho.
- *Vulnerability Analysis:*  
Uma vez tendo os métodos de ataque definidos é necessário realizar teste para definir quais formas são as mais viáveis de se chegar aos objetivos dos ataques. Este é um tipo de fase usada neste trabalho.

- *Exploitation:*

É nela que de fato acontecem as tentativas de burlar a segurança do sistema baseado nas vulnerabilidades listadas anteriormente.

- *Post Exploitation:*

Nesta fase determina-se quão graves são as falhas encontradas, é preciso pensar como um *Cracker* para dimensionar o quão perigosa a falha pode se tornar para o cliente.

- *Reporting:*

Como o próprio nome já diz, nessa fase são reportadas todas as falhas e as dimensões que essas podem tomar caso não sejam tratadas.

Essas fases garantem ao profissional que não deixe escapar nenhum detalhe antes de realizar suas tentativas de ataque e devolva ao cliente uma documentação detalhada de como os teste se sucederam.

## 2.9 ATAQUES

De acordo com Ulbrich e Della Valle (2004, p.125), existem dois principais tipo de ataques, o direto e o indireto, onde muitas vezes é necessário um pouco dos dois para se conseguir o resultado esperado.

### 2.9.1 ATAQUE DIRETO

É o tipo de ataque que se caracteriza por contato direto com a vítima segundo Ulbrich e Della Valle (2004, p.125). Esse contato pode ser via telefone, e-mail ou mesmo pessoal, requerendo planejamento prévio, boa articulação para que o atacante evite ser *desmascarado* e raciocínio rápido para as mais variadas situações.

### 2.9.2 ATAQUE INDIRETO

Ainda Ulbrich e Della Valle (2004, p.125) definem o ataque indireto como a utilização de ferramentas de invasão (como cavalos de tróia e sites com código malicioso) e de



impostura (como cartas, e-mails e sites falsos com a aparência dos verdadeiros) para obter informações pessoais. Os usuários individuais de quem o *hacker* extrai os dados são apenas vetores para a coleta de informações de uma entidade maior - empresa, organização ou governo. Sua intenção não é atacar cada um desses usuários, e sim o organismo maior ao qual elas pertencem”.

### **2.9.3 COLETA DE INFORMAÇÃO**

“Para chegar à abordagem direta, o invasor deve ter conseguido uma bela coleção de informações[...]”, Ulbrich e Della Valle (2004, p.125).

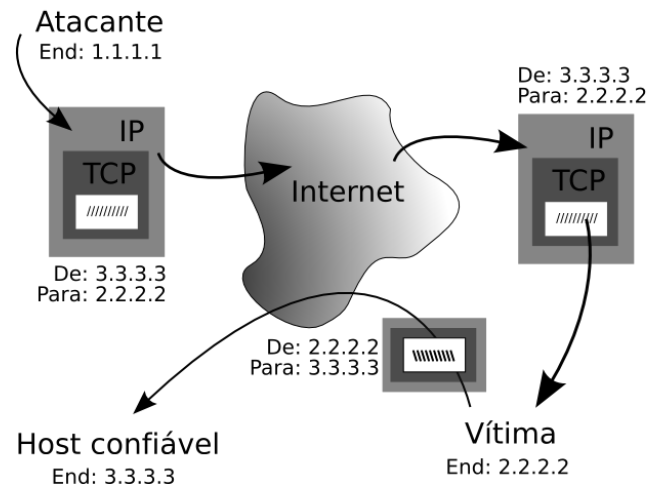
De forma similar Andress e Linn (2012, p.201) afirmam que a coleta de informação e pesquisa pode ser de grande valor para os testes de penetração, uma vez que não se tem muitas informações sobre o alvo ou ambiente.

### **2.9.4 SPOOFING**

Segundo Da Costa (2013, p.22), *spoofing* é uma técnica cuja o invasor se passa pela vítima afim de adquirir suas permissões, acessando o que não deveria.

De maneira análoga Tâmega (2003, p.37) afirma que a técnica do *spoofing* envolve o fornecimento de informações falsas sobre a vítima, adquirindo acesso não autorizado e ainda alterando a forma que o cliente e o servidor se comunicam.

A imagem 2.2.2 ilustra o conceito do *spoofing*.

Figura 2.2.2 - *Spoofing*

Fonte: [upload.wikimedia.org/wikipedia/commons/7/7d/IP\\_spoofing.png](https://upload.wikimedia.org/wikipedia/commons/7/7d/IP_spoofing.png)

### 2.9.5 SNIFFING

Para Erikson (2008, p.224), pacotes de dados trafegam pela rede visitando todos os dispositivos conectados à ela, esperando que apenas aqueles que são destinatários recebam. O *Sniffer* consiste em um dispositivo em modo *promíscuo*, de forma que ele obtenha todos os pacotes que navegam pela rede. Existem vários programas que utilizam essa técnica, porém poucas configurações são capazes de ligar o modo *promíscuo* de um computador comum, como é mostrado na figura 2.2.3.

Figura 2.2.3 - Modo Promíscuo

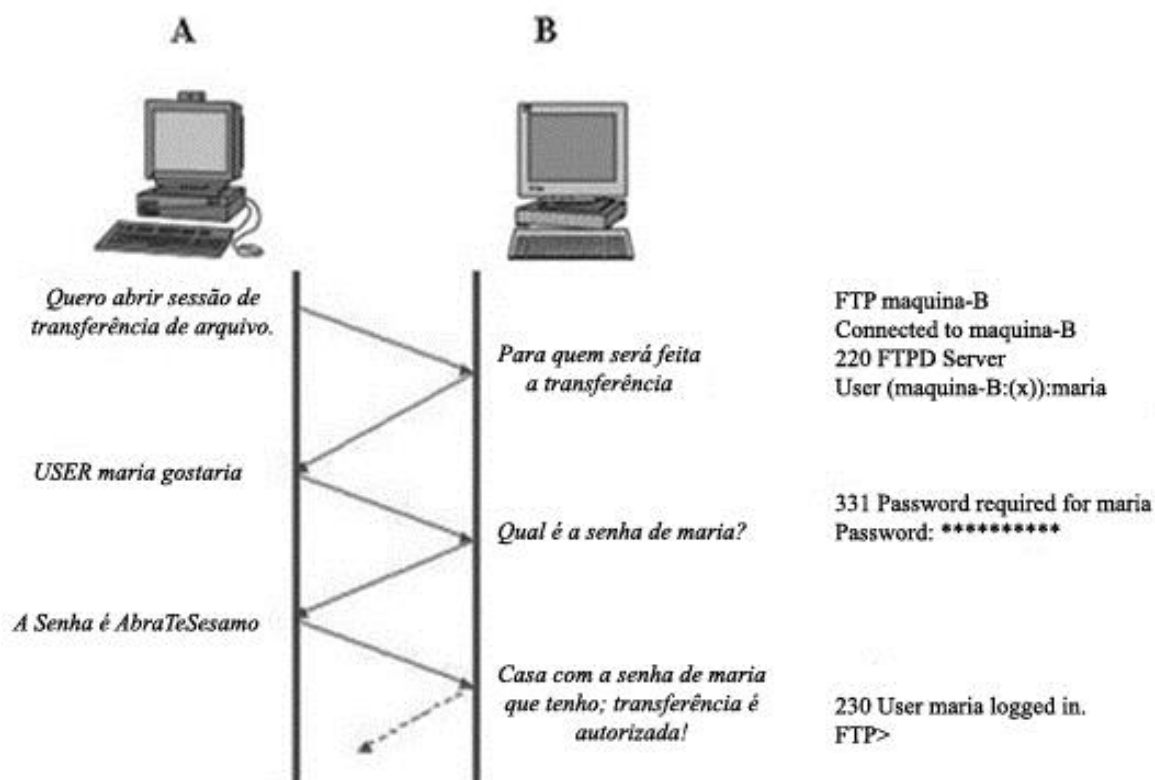
```
leon@leon-N46VM:~$ ifconfig wlan0
wlan0      Link encap:Ethernet  HWaddr dc:85:de:1e:cb:15
            inet addr:192.168.25.5  Bcast:192.168.25.255  Mask:255.255.255.0
            inet6 addr: fe80::de85:deff:fe1e:cb15/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:1540868 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1580854 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:1000589613 (1.0 GB)  TX bytes:451340372 (451.3 MB)

leon@leon-N46VM:~$ sudo ifconfig wlan0 promisc
leon@leon-N46VM:~$ ifconfig wlan0
wlan0      Link encap:Ethernet  HWaddr dc:85:de:1e:cb:15
            inet addr:192.168.25.5  Bcast:192.168.25.255  Mask:255.255.255.0
            inet6 addr: fe80::de85:deff:fe1e:cb15/64 Scope:Link
            UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
            RX packets:1541019 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1581001 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:1000640651 (1.0 GB)  TX bytes:451410512 (451.4 MB)
```

Fonte: **Hacking: The Art Of Exploitation**, No Starch Press 2008(alterado pelo autor)

Da Costa (2013, p.23), define *Sniffers* como programas que monitoram a atividade, registrando todo o fluxo de dados que trafega pela rede, podendo interceptar informações importantes, tais como acessos à emails, acesso remoto (VPN), arquivos (FTP), etc. Na figura 2.2.4 o "farejador" captura todo o fluxo de dados que ocorreu entre o computador A e o computador B, conseguindo o usuário e a senha da vítima.

Figura 2.2.4 - Sniffing



Fonte: Segurança em Redes de Computadores.

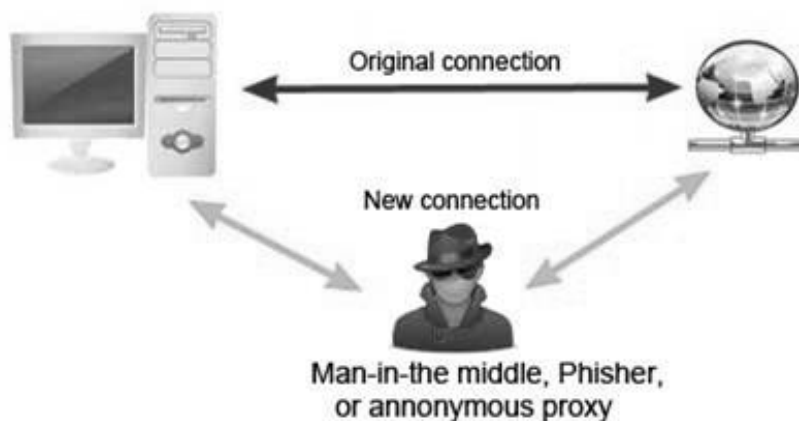
### 2.9.6 MITM - MAN-IN-THE-MIDDLE

Segundo Erikson (2008, p.406) o ataque *MitM* se caracteriza por um atacante entre dois dispositivos da rede (terminais, servidores, etc), de forma que cada dispositivo da rede acredite que esta se comunicando com a outra, quando na verdade o atacante recebe e envia suas mensagens, podendo alterar, copiar ou até mesmo deletar as mesmas.

Ainda Erikson (2008, p.407) afirma que quando uma conexão encriptada é estabelecida, uma chave secreta é gerada e transmitida usando cifras assimétricas, sendo usada para comunicar as duas partes, essa técnica previne que qualquer *Sniffer* consiga entender o que está sendo transmitido.

Muito embora, o ataque *MitM* faz com que ambas as partes de uma comunicação acreditem de fato que estão comunicando-se entre si, de forma que as chaves são compartilhadas com o atacantes, garantindo que este decifre suas mensagens tornando-as legíveis. A figura 2.2.5 ilustra a ideia de um ataque *MitM*, onde o atacantes se posiciona entre as duas partes de uma comunicação.

Figura 2.2.5 - MitM



Fonte: [computerhope.com/jargon/m/maninthemiddleattack.jpg](http://computerhope.com/jargon/m/maninthemiddleattack.jpg).

### 2.9.7 DOS - DENIAL OF SERVICE

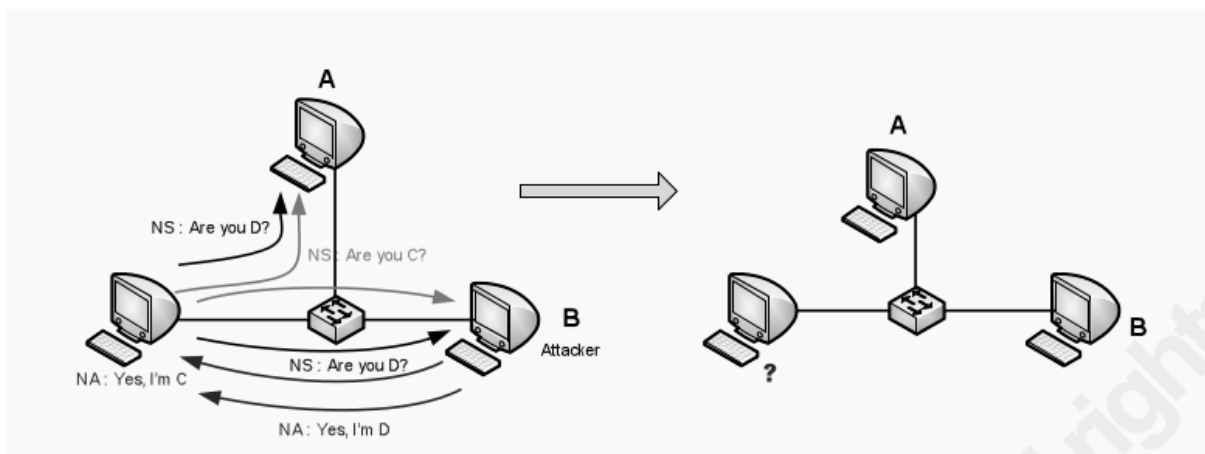
De acordo com a definição do US-CERT (United States Computer Emergency Readiness Team)(ST04-015), DoS é um tipo de uma técnica onde o atacante previne a conexão de um usuário legítimo à uma rede.

De forma similar Erikson (2008, p.251) divide os ataques DoS em dois tipos: *Crash services* e *Flood services*.

O tipo *Crash service* visa interromper um serviço utilizando algum *exploit* (*buffer overflow* por exemplo), impedindo que usuários comuns conectem à ele.

O *Flood service* por sua vez evita que usuários conectem ao um serviço simulando uma rede lotada, trazendo à exaustão dos IPs disponíveis.

Figura 2.2.6 - DoS



Fonte: **Attacking the IPv6 protocol suite**, p.63 THC 2008.

A figura 2.2.6 mostra um ataque DoS do tipo *Flood service*, onde o atacante (computador B) se apresenta como se fosse o computador B, C, D e qualquer outro que o computador A perguntar, encontrando então uma rede lotada, onde nenhum IP será disponibilizado à ele.

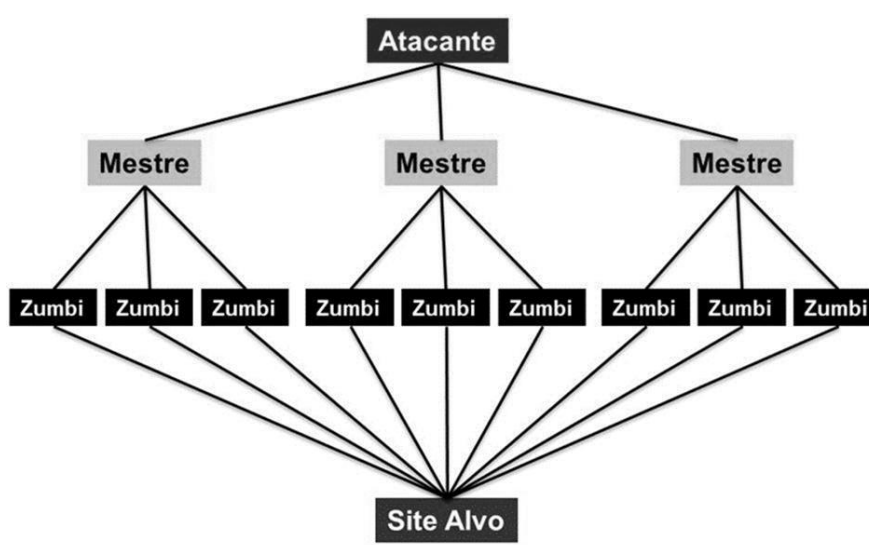
### 2.9.8 DDOS - DISTRIBUTED DENIAL OF SERVICE

O US-CERT(ST04-015) define DDoS como uma grande quantidade de computadores enviando muitos dados para um destino específico, tornando então o serviço inoperante.

Erikson (2008, p.258) cita o DDoS como um DoS de tipo *Flood service*, uma vez que seu objetivo é a exaustão de recursos, usando de vários computadores para exaurir os recursos deste.

Segundo Costa (2013, p.30) os computadores de usuários que são infectados com vírus do tipo DoS passam a ser chamados de computadores *zumbis*, contactando com computadores chamados de *Mestres*, que recebem comando do atacante (em que período e qual destino executar), enviando então grandes quantidades de dados para um único destino ao mesmo tempo, como é mostrado na figura 2.2.7.

Figura 2.2.7 - DDoS



Fonte: **Segurança em Redes de Computadores.**

## 2.10 SEGURANÇA NO IPV6

Os tipos de ataques ao IPv6 também sofreram mudanças de acordo com Florentino (2012, p.82). Varreduras por portas abertas, por exemplo, se torna uma prática impossível, uma vez que este fornece uma quantidade muito grande de combinações, “para se ter uma ideia da quantidade de IPs possíveis em uma rede /64 com 264 combinações de *hosts* possíveis, mesmo percorrendo 1 milhão de endereços por segundo, seriam necessários mais de 500.000 anos para se percorrer toda a sub-rede”.(Florentino, 2012).

Como já foi discutido, apesar do protocolo IPv6 apresentar muitas vantagens, suas vulnerabilidades causam preocupação. De acordo com Pilihanto (2011, p.2) pesquisadores já publicaram ferramentas para testes de penetração no IPv6.

Van Hauser do *The Hacker Choice* (THC, 2014) disponibilizou uma ferramenta citada por muitos autores o *THC IPv6 Toolkit*, que apresenta diversos algoritmos que usam dessas vulnerabilidades do IPv6 para o *PenTest*.

### 2.10.1 THC IPV6 TOOLKIT

De acordo com o site da THC, o kit é um conjunto de ferramenta que exploram as vulnerabilidades do IPv6 e ICMP6, para este estudo foram selecionados 3, que são os mais conhecidos, *parasite6*, *dos-new-ip6*, *flood\_router6*.

- *parasite6*: Utiliza o ICMP neighbor solicitation/advertisement spoofer, é um tipo de ataque *man-in-the-middle*, assim como o ARP MITM.
- *alive6*: Muito efetivo para escanear todos os IPv6 presentes em uma rede, lista todos os sistemas que estão *escutando* a interface.
- *fake\_router6*: Posiciona o atacante como Router na rede, com a mais alta prioridade.
- *detect-new-ip6*: Detecta novos dispositivos que acessam a rede, é possível criar scripts para escanear esses sistemas automaticamente.
- *dos-new-ip6*: Detecta novos dispositivos que acessam a rede assim como o *detect-new-ipv6*, porém se diz usuário de todos os IPv perguntados à rede, evitando que o novo sistema acesse a rede.
- *flood\_router6*: “Inunda” a interface com *router advertisements* randômicos, incapacitando os sistemas conectados à ela.
- *flood\_advertise6*: “Inunda” a interface com *neighbor advertisements* randômicos, incapacitando os sistemas conectados à ela.
- *fake\_advertiser6*: Anuncia o atacante na rede.



## CAPÍTULO 3 METODOLOGIA

Em um primeiro momento foi realizado um levantamento de dados com base em pesquisas sobre as vulnerabilidades do IPv6.

Após o levantamento das vulnerabilidades foi elaborado um laboratório virtual para os testes, afim de documentar o comportamento de cada sistema mediante determinado ataque.

O laboratório visa simular um ambiente de rede real, composto por 4 (quatro) componentes, sendo 1 (um) atacante e 3 (três) vítimas.

O objetivo dos testes foi levantar dados que permitam uma perspectiva de como as vulnerabilidades do IPv6 se comportam em cada sistema.

Para cada vulnerabilidade testada foi proposta uma solução para a mesma. A tabela abaixo lista as ferramentas utilizadas no estudo de vulnerabilidades.

Quadro 1 - Ferramentas utilizadas

Ferramenta escolhida	Necessidade
Intel Core i7-3610 8GB de memória RAM 1TB de armazenamento	Hardware
Windows 7 Windows XP Kali Linux Ubuntu Linux	Sistemas operacionais
VirtualBox 4.3.22	Virtualizador
WireShark	Sniffer

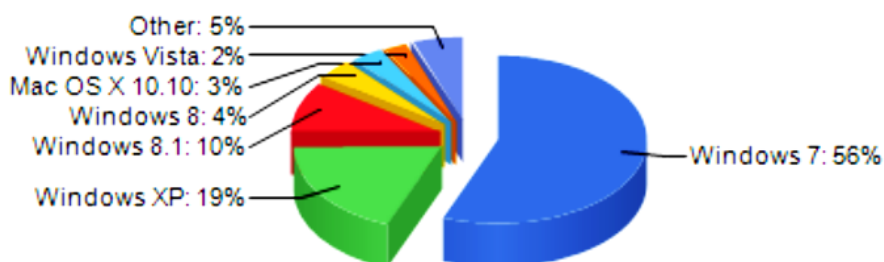
Fonte: Autor

Por se tratar de uma virtualização não foram necessários diversos dispositivos para realizar os testes, apenas um computador de bom desempenho.

- Processador: Intel® Core™ i7-3610QM 2.30GHz × 8
- Memória: 8 Gb
- HD: 1 Tb

Os sistemas operacionais que compuseram o laboratório virtual foram selecionados a partir do ranking do site *netmarketshare.com* referente ao mês de janeiro de 2015. Onde indica os sistemas operacionais desktop mais utilizados atualmente, como é mostrado na figura 3.1.1.

Figura 3.1.1 - Sistemas Operacionais mais usados

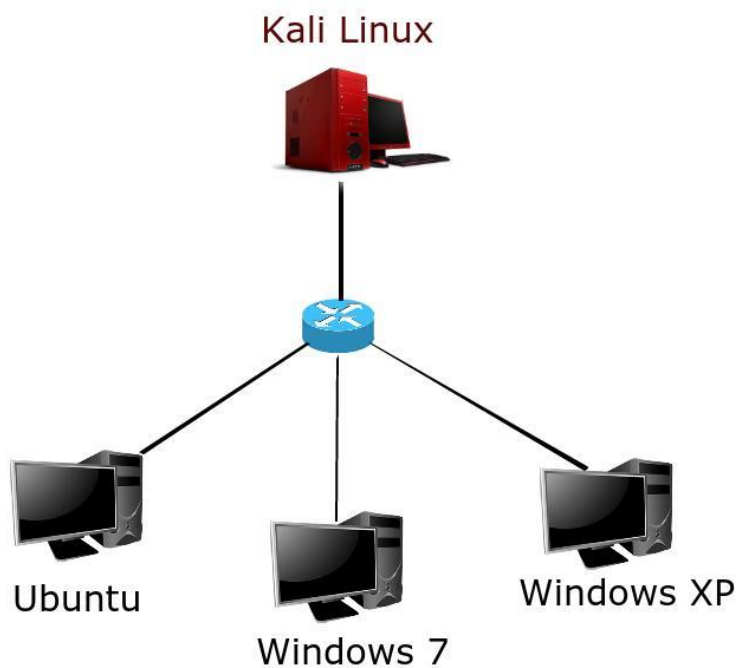


Fonte: [netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0&qptimeframe=Y](http://netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0&qptimeframe=Y).

Como os sistemas Windows são os mais utilizados atualmente, com aproximadamente 91% do mercado de desktop, foram escolhidos os dois com maior porcentagem de uso, além de uma arquitetura diferente à da Microsoft. Nesse caso foi selecionado o sistema operacional Kali Linux, devido ao seu grande foco em segurança para executar os ataques e o Ubuntu para atuar como vítima junto aos Windows 7 e XP.

O laboratório ficou composto como na figura 3.1.2.

Figura 3.1.2 - Laboratório para testes



Fonte: Autor

Para simular a rede foi utilizado o virtualizador Virtual Box 4.3.22 devido à sua grande popularidade e simplicidade de uso.

Para simular os ataques de MitM foi escolhida a ferramenta *WireShark* para ajudar a visualizar os pacotes que trafegaram pela rede.

## CAPÍTULO 4 TESTES DE ATAQUES

Com base em pesquisas foi proposto a realização de 3 (três) tipos de ataques bastante populares, o *Flood*, *DOS* e *MITM*.

O estudo buscou analisar como é explorada a vulnerabilidade do protocolo IPv6 para executar os ataques.

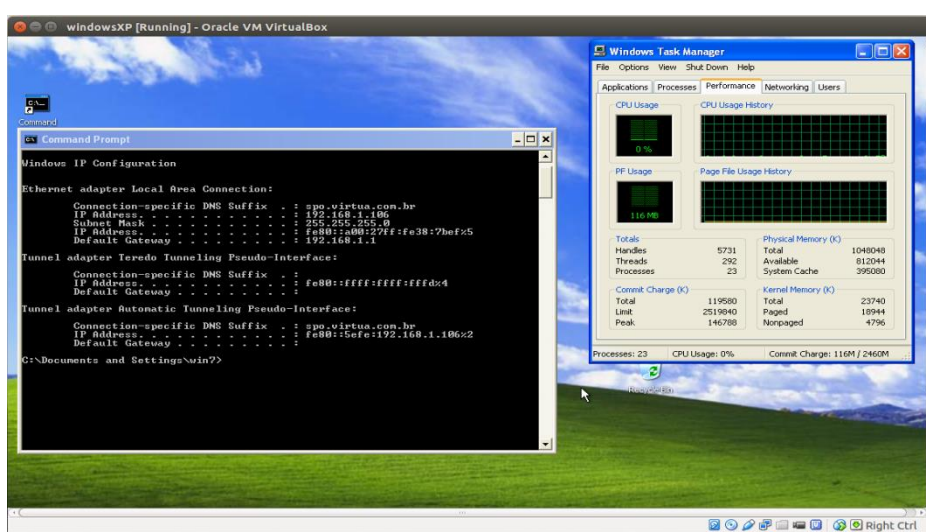
### 4.1 FLOOD

Para o teste do ataque de *Flood* foi utilizada a ferramenta *flood\_router6* do kit THC-IPv6 ToolKit.

Nesse tipo de ataque o sistema Kali anuncia um novo roteador na rede com alta frequência, de forma que sejam enviados *router advertisements* à todos os dispositivos da rede, o IPv6 permite que cada dispositivo responda ao roteador diretamente, porém se muitos roteadores enviam e solicitam resposta o dispositivo pode não suportar essa carga e parar de funcionar. É exatamente esse comportamento que se esperava das máquinas vitimas.

O computador Windows XP não possui o IPv6 configurado com padrão, de forma que foi necessário utilizar o comando *netsh int ipv6 install*, que facilmente torna o sistema pronto para o uso do IPv6, que ficou como mostrado pela figura 3.1.3.

Figura 3.1.3 - Windows XP antes do ataque

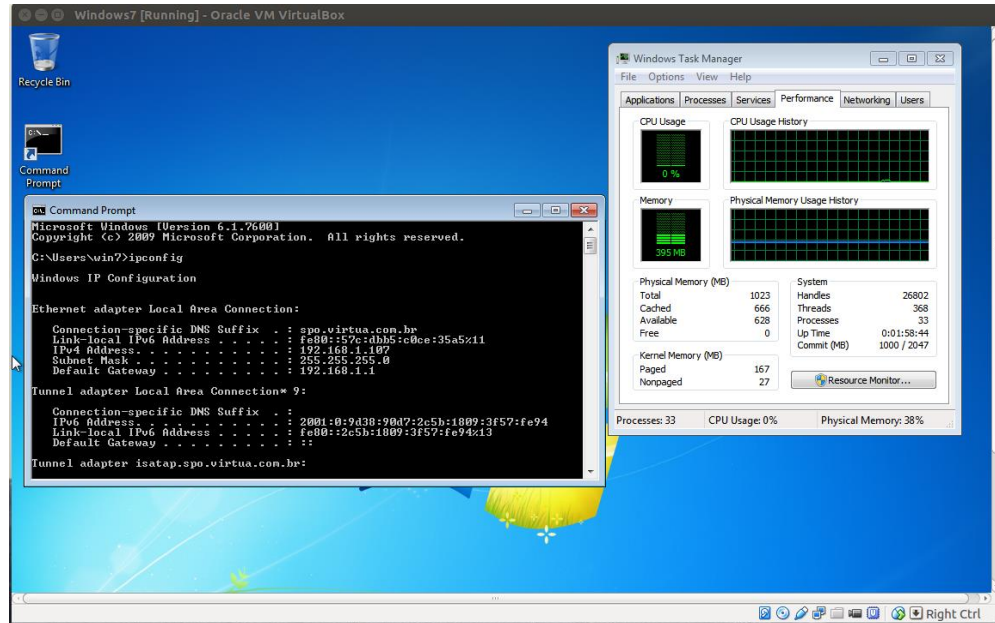


Fonte: Autor

Pode-se perceber que o dispositivo possui dois *IP address*, um IPv4 e outro IPv6.

O sistema Windows 7 estava configurado como mostra a figura 3.1.4.

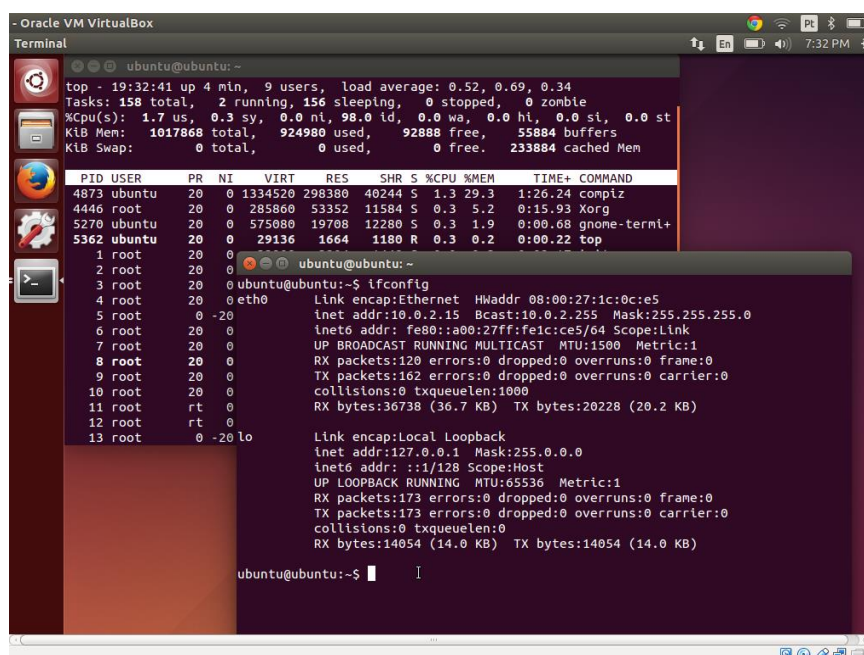
Figura 3.1.4 - Windows 7 antes do ataque



Fonte: Autor

O comando *ifconfig* na plataforma linux é análogo ao *ipconfig* da plataforma Microsoft, o sistema Ubuntu apresentou sua configuração como ilustra a figura 3.1.5.

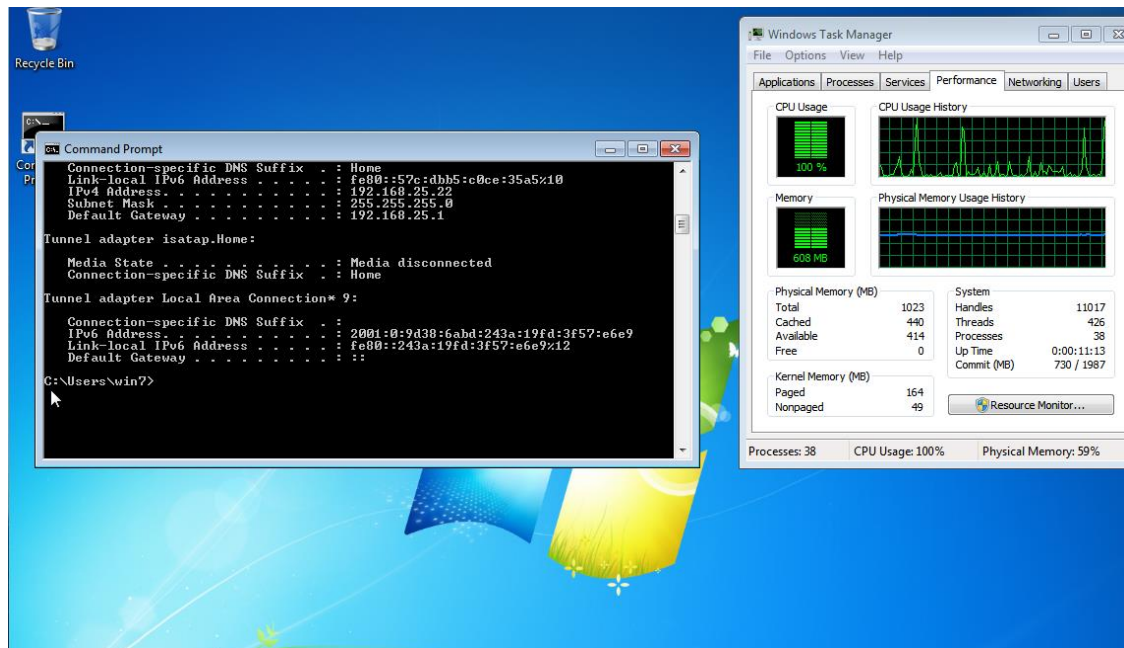
Figura 3.1.5 - Ubuntu antes do ataque



Fonte: Autor



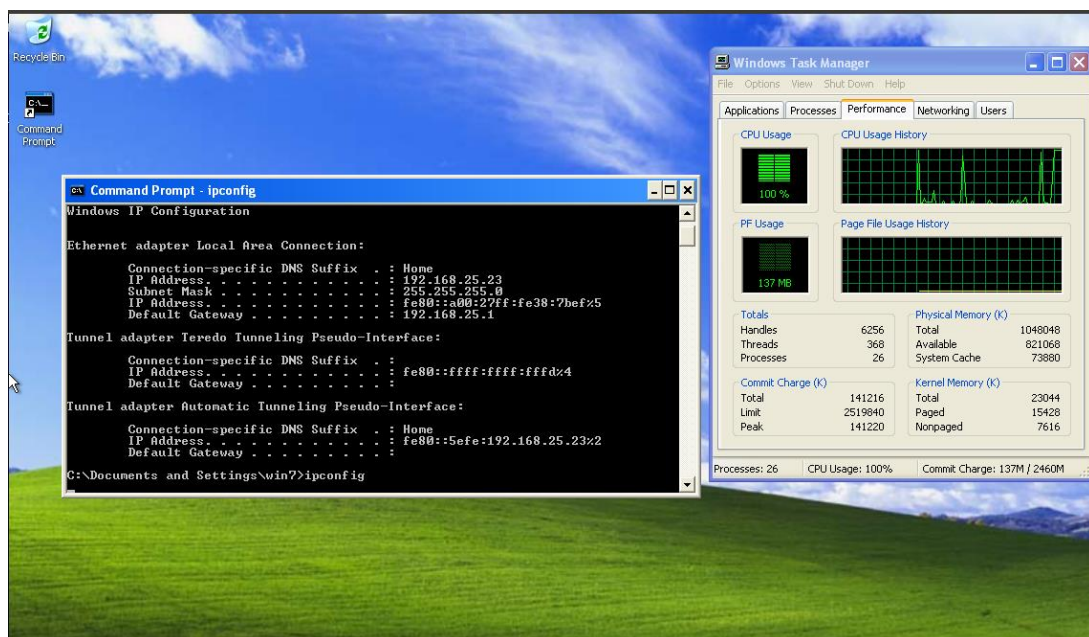
Figura 3.1.7 - Windows 7 durante ataque flood\_router



Fonte: Autor

O sistema Windows XP apresentou o mesmo resultado que o Windows 7; intenso uso de CPU e paralisa em poucos segundos, como mostra a figura 3.1.8.

Figura 3.1.8 - Windows XP durante ataque flood\_router

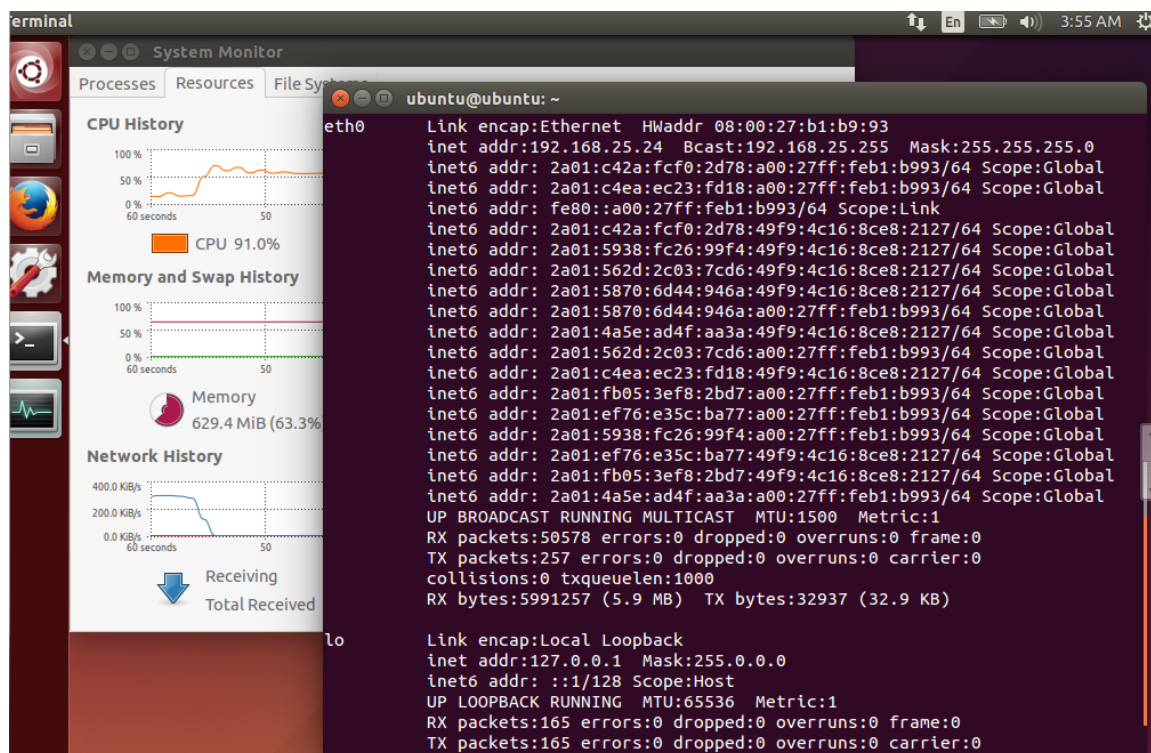


Fonte: Autor



O sistema Ubuntu por sua vez não demonstrou reação negativa, seu alto uso de CPU se referia à outros processos, mantendo-se constante durante a execução do ataque, como mostram a figura 3.1.9.

Figura 3.1.9 - Ubuntu durante ataque flood\_router



Fonte: Autor

A causa do sistema Ubuntu não ter reagido ao ataque se deve ao fato de sistemas Linux permitirem no máximo 17 roteadores conectados ao sistema ao mesmo tempo, de forma que o ataque de *flood* se torna ineficaz.

## 4.2 DOS

Para o teste do ataque de *DoS* foi utilizada a ferramenta *dos-new-ip6* do kit THC-IPv6 ToolKit.

Nesse ataque o sistema Kali fez uso de um conceito de conexão do IPv6 bastante simples. Para um novo dispositivo se conectar à rede, um novo IP deve ser gerado para ele, de forma que é perguntado à cada terminal se este possui o IP que se pretende ser designado ao novo dispositivo através do *ICMPv6 neighbor solicitation*. Esse ataque consiste em responder, independentemente do IP perguntado, que o atacante faz uso do IP, de forma que o

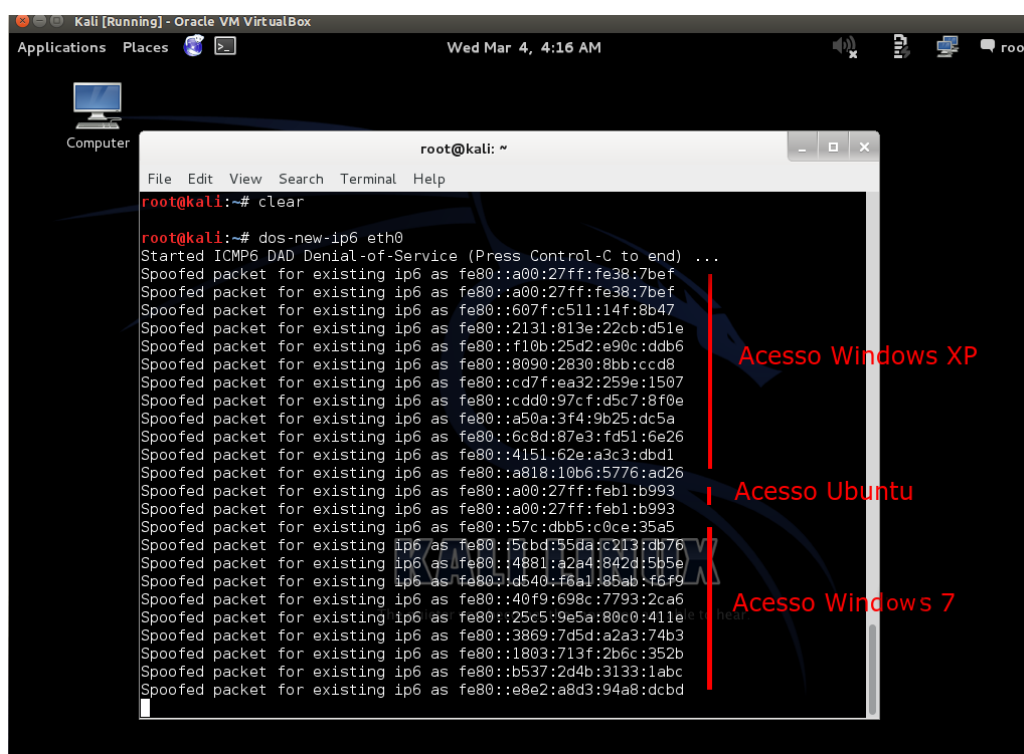


novo dispositivo nunca conseguirá ter acesso à conexão IPv6, uma vez que todos IPs perguntados estão em uso.

O processo de teste foi o mesmo que o anterior, ou seja, a configuração antes do ataque é a mesma mostrada nas figuras 3.1.3, 3.1.4 e 3.2.5.

O sistema Kali linux se anunciou como 24 endereços de IP na rede, a figura indica em que momento cada componente da rede tentou se conectar via IPv6, como mostra a figura 3.2.1.

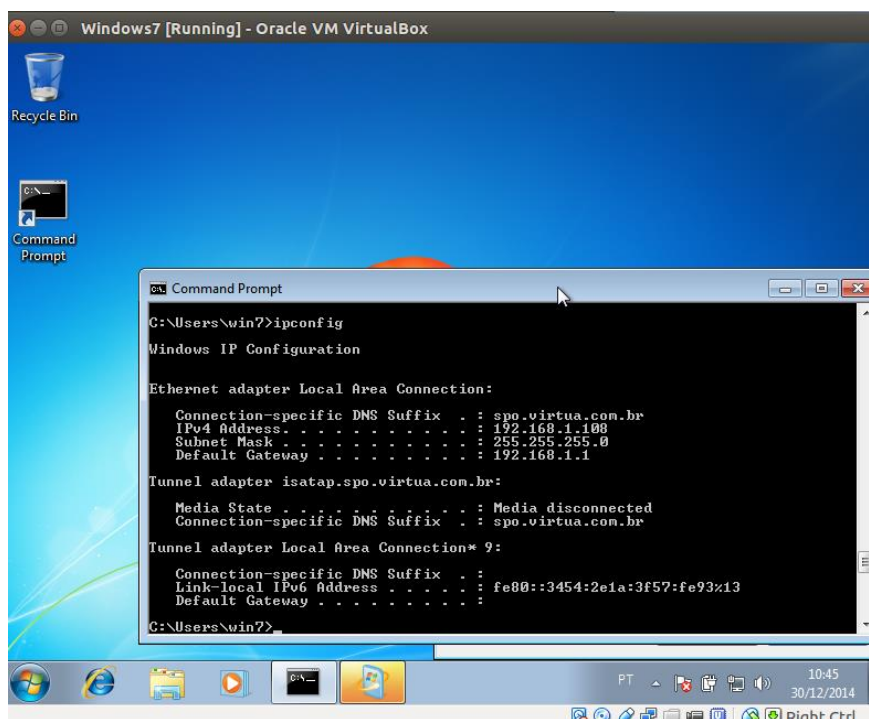
Figura 3.2.1 - Kali Linux durante ataque DoS



Fonte: Autor

O ataque foi efetivo no sistema Windows 7 que não mostrou um endereço IPv6 após a execução, como ilustra a figura 3.2.2.

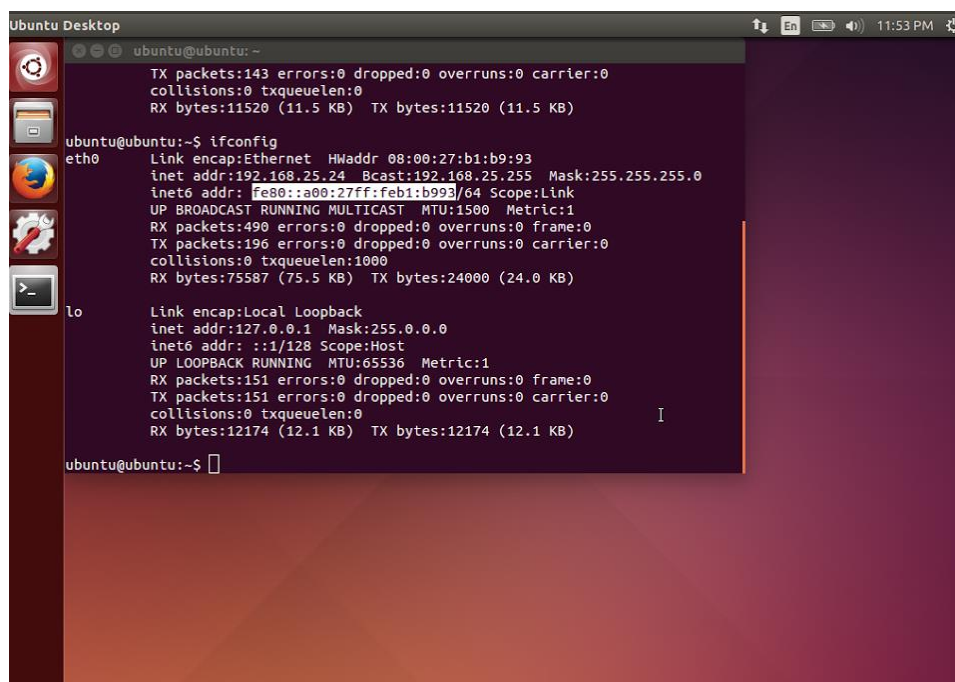
Figura 3.2.2 - Windows 7 durante ataque DoS



Fonte: Autor

O Sistema Ubuntu não demonstrou reação ao ataque *DoS*, adquirindo um endereço IPv6 mesmo com este sendo anunciado pelo Kali, como visto na figura 3.2.3.

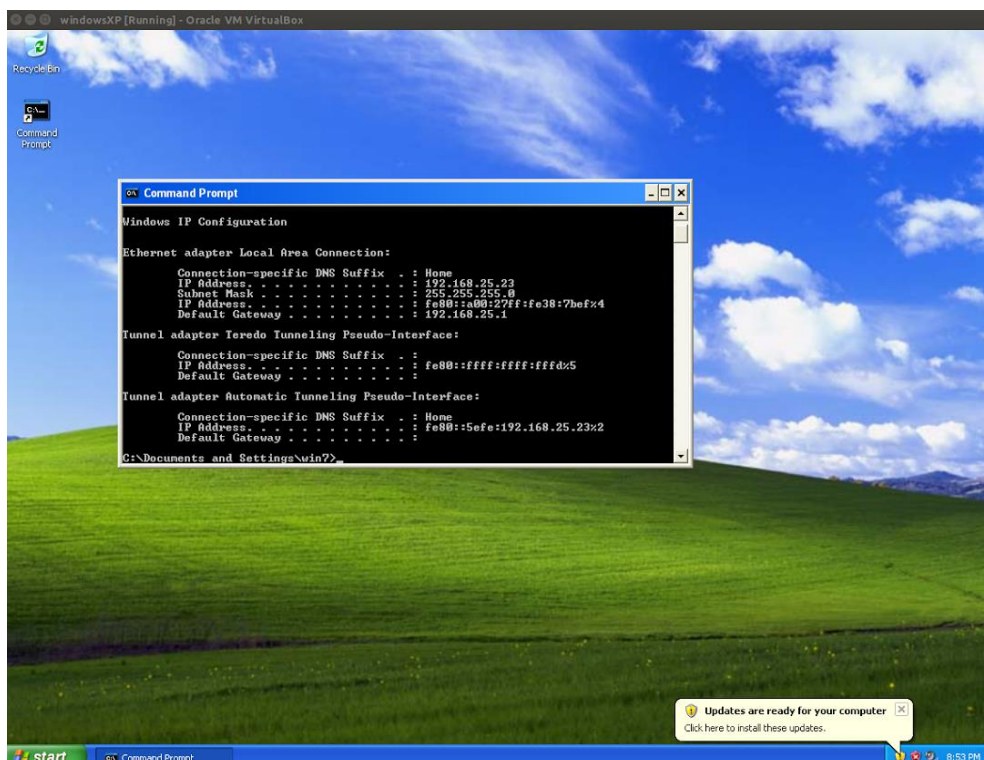
Figura 3.2.3 - Ubuntu durante ataque DoS



Fonte: Autor

De forma análoga o Sistema Windows XP também não demonstrou reação ao ataque *DoS*, o IP por ele adquirido também foi anunciado pelo Kali, como mostra a figura 3.2.4.

Figura 3.2.4 - Windows XP durante ataque DOS



Fonte: Autor

### 4.3 MITM

Para o teste do ataque de *MitM* foi utilizada a ferramenta *pirasite6* do kit THC-IPv6 ToolKit.

O processo de testes foi similar aos anteriores, todos os sistemas se comportaram de forma análoga.

Foi executado uma ferramenta do kit THC-IPv6 ToolKit chamada *alive6*, cuja lista os endereços de IPv6 disponíveis na rede, como mostra a figura 3.2.5.

Figura 3.2.5 - Kali Linux alive6

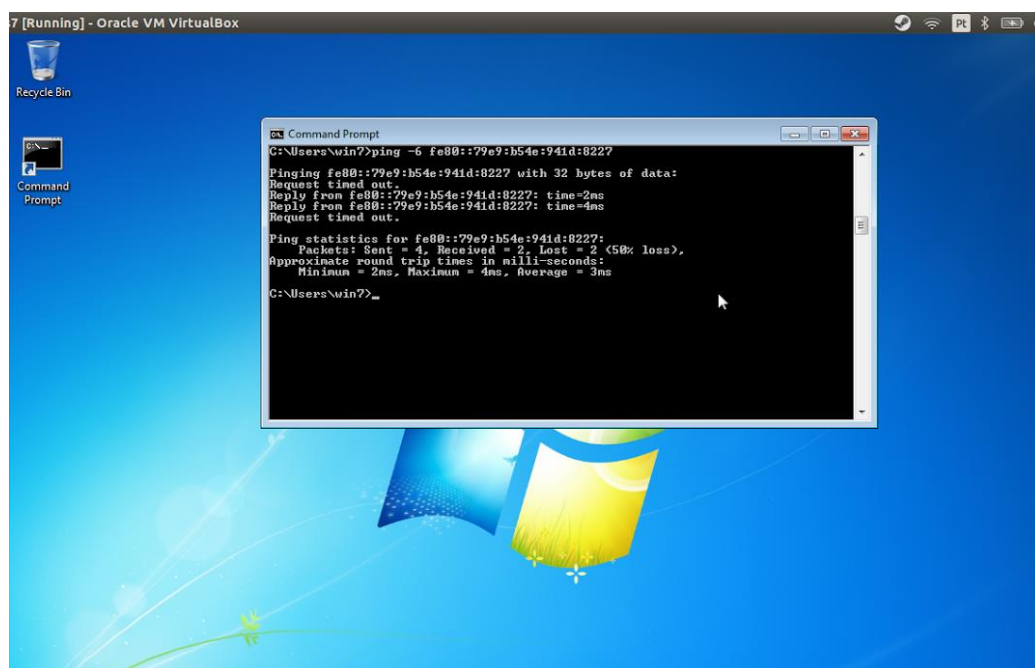
```
root@kali:~# alive6 -l eth0
Alive: fe80::de85:deff:fe1e:cb15 [ICMP echo-reply]
Alive: fe80::57c:dbb5:c0ce:35a5 [ICMP parameter problem]
Alive: fe80::6a15:90ff:fe47:ab4d [ICMP echo-reply]
Alive: fe80::79e9:b54e:941d:8227 [ICMP parameter problem]
Alive: fe80::cec3:eaff:fea9:228a [ICMP echo-reply]

Scanned 1 address and found 5 systems alive
```

Fonte: Autor

Com a lista de IPs “vivos” na rede, foi executado um simples comando *ping -6* nas vítimas (windows XP, 7 e Ubuntu) para verificar se o Kali foi capaz de capturar o fluxo de dados, como ilustra a figura 3.2.6.

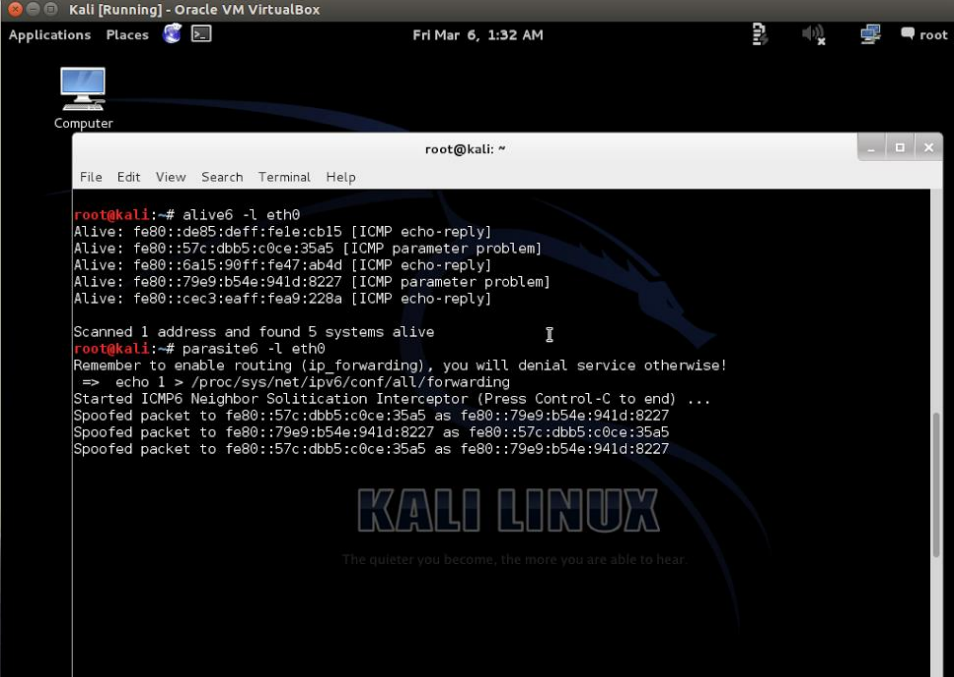
Figura 3.2.6 - Windows 7 Ping -6



Fonte: Autor

O procedimento “pingou” 2 pacotes para um dos IPs contidos na lista, de forma que foi possível verificar o tráfego pelo sistema Kali Linux, que recebia os pacotes do remetente e reenviava ao destinatário, como é visível pela figura 3.2.7.

Figura 3.2.7 - Kali Linux parasite6



The image shows a Kali Linux terminal window titled "Kali [Running] - Oracle VM VirtualBox". The terminal output shows the execution of the `alive6` and `parasite6` tools. The `alive6` command scans for alive systems on the `eth0` interface, finding five systems. The `parasite6` command then initiates an ICMP6 Neighbor Solicitation Interceptor, spoofing packets to the discovered systems. The terminal background features the Kali Linux logo and the slogan "The quieter you become, the more you are able to hear."

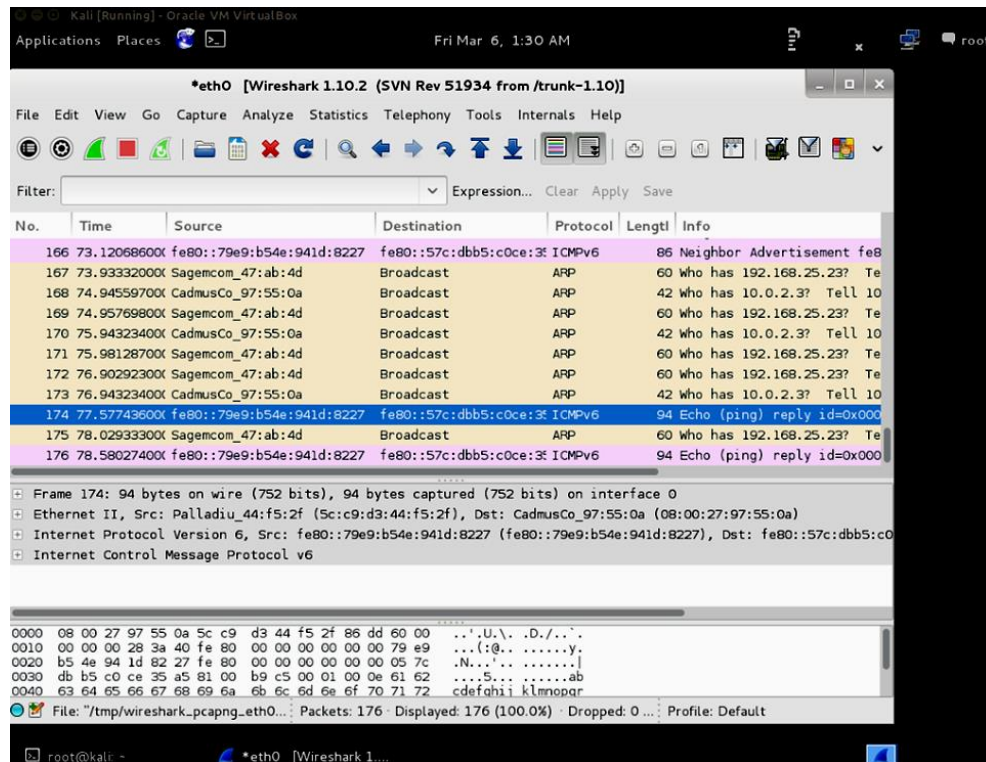
```
root@kali:~# alive6 -l eth0
Alive: fe80::de85:deff:fe1e:cb15 [ICMP echo-reply]
Alive: fe80::57c:dbb5:c0ce:35a5 [ICMP parameter problem]
Alive: fe80::6a15:90ff:fe47:ab4d [ICMP echo-reply]
Alive: fe80::79e9:b54e:941d:8227 [ICMP parameter problem]
Alive: fe80::cec3:eaff:fea9:228a [ICMP echo-reply]

Scanned 1 address and found 5 systems alive
root@kali:~# parasite6 -l eth0
Remember to enable routing (ip_forwarding), you will denial service otherwise!
=> echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
Started ICMP6 Neighbor Solicitation Interceptor (Press Control-C to end) ...
Spoofed packet to fe80::57c:dbb5:c0ce:35a5 as fe80::79e9:b54e:941d:8227
Spoofed packet to fe80::79e9:b54e:941d:8227 as fe80::57c:dbb5:c0ce:35a5
Spoofed packet to fe80::57c:dbb5:c0ce:35a5 as fe80::79e9:b54e:941d:8227
```

Fonte: Autor

Através da ferramenta *WireShark* foi verificado a natureza do tráfego de rede, que de fato se tratou de um *ping*, como apresenta a imagem 3.2.8.

Figura 3.2.8 - Kali Linux Wireshark



Fonte: Autor



## CAPÍTULO 5 RESULTADOS

A partir dos testes realizados neste estudo, foi possível extrair uma tabela que ilustra a reação de cada sistema diante determinado ataque. O quadro 2, exibe a eficácia do ataque em cada sistema operacional.

Quadro 2 - Resultados

	MitM	DoS	Flood
Windows XP	<b>Eficaz</b>	Ineficaz	<b>Eficaz</b>
Windows 7	<b>Eficaz</b>	<b>Eficaz</b>	<b>Eficaz</b>
Ubuntu	<b>Eficaz</b>	Ineficaz	Ineficaz

Fonte: Autor

O ataque *flood* se comportou como esperado, uma vez que foi possível observar perfeitamente a quantidade limitada de roteadores permitida pelo sistema Linux, garantindo seu funcionamento e o colapso do sistema Windows. Uma contramedida para o ataque de *flood* seria o total desligamento do IPv6 ou o uso de um *IDS* para detectar anomalias na rede.

O ataque *DoS* não funcionou como esperado, ainda considerando que os sistemas Windows possuem arquitetura similar, a versão 7 de fato não adquiriu acesso ao IPv6 enquanto a versão XP pareceu ignorar a existência do IPv6 perguntando, isso se deu ao fato de que a versão XP não determina regras diferentes entre o IPv4 e o IPv6, ou seja, o firewall apenas abre portas para o IPv4 ou apenas bloquear o ICMP do IPv6. Comportamento similar foi observado no sistema Ubuntu, que utilizou o mesmo IPv6 perguntado ao Kali, isso se deve à uma característica particular dos sistemas Linux, que avisa para duplas detecções de endereço, o que indica um *DoS* em curso, dessa forma o administrador da rede pode simplesmente executar o comando `sysctl net.ipv6.conf.wlan0.accept_dad=0`, configurado por padrão.

Assim como o *flood*, o ataque *MitM* também se comportou como esperado, todos os sistemas tiveram seus tráfegos capturados pelo *parasite6* em sua execução.

Todos os ataques executados pelo sistema Kali Linux apresentaram uma grande facilidade de execução, uma vez que um só comando era o suficiente. O ataque *MitM* foi o único que necessitou de uma ferramenta auxiliar para visualizar tráfego da rede e o que se passava por ele.

## CAPÍTULO 6 CONCLUSÕES

A mais nova versão do protocolo de internet IPv6 possui um grande espaço de endereçamento e diferenças em seu cabeçalho em relação ao seu predecessor IPv4. Essas diferenças impactam na segurança de rede, tanto para o administrador quanto para o atacante.

Devido ao grande número de endereços proporcionados pelo IPv6, alguns dos ataques já conhecidos no IPv4 se tornam inviáveis. Varreduras de uma rede /24 tomava alguns minutos do atacante, mas redes /64 no IPv6 inviabilizam o ataque.

Ferramentas usadas para atacar o IPv6 devem ser reconfiguradas afim de atender ao seu novo cabeçalho, assim como os cuidados por parte do administrador também deve mudar, considerando a amplitude do protocolo. As técnicas de transição do IPv4 para o IPv6 também são uma fonte de preocupação para a segurança.

Os conceitos de ataques no IPv6 pouco mudam em relação ao seu predecessor IPv4 como foi observado no estudo. Ataques como *Flood*, *DoS* e *MitM* possuem as mesmas características, diferem em suas implementações para atender mudanças na estrutura do cabeçalho.

Novos esforços precisam ocorrer para manter a segurança do protocolo IPv6, por se tratar de um protocolo novo muitas lacunas serão encontradas e devem ser preenchidas para garantir a segurança dos dados transportados.

Em relação ao IPv4 o novo protocolo IPv6 não se mostrou mais vulnerável, nem menos. Ambos possuem características que protegem e expõem pontos fracos, de forma que não é possível afirmar neste trabalho que por se tratar de uma nova tecnologia o IPv6 é mais seguro.

Futuramente é pretendido continuar pesquisando acerca de novas vulnerabilidades e fraquezas encontradas no protocolo IPv6, sua implementação ainda é tímida comparada ao de seu antecessor, é nítido que muito ainda será descoberto sobre ele. Um acompanhamento é necessário por todos que o utilizam em seus negócios ou usam para testes de penetração.

Foi percebido por essa pesquisa que os ataques *flood* são eficazes contra sistemas Windows. Ataques de *DoS* são eficazes apenas para o Windows 7 dentre os analisados e o ataque *MitM* é eficaz para todas as plataformas.

O IPv6 é uma tecnologia que será empregada por todos em um futuro próximo, por esse motivo pesquisas como essa são vitais para uma melhor adesão de sua implementação.



## REFERÊNCIAS

- ANDRESS, Jason; LINN, Ryan. **Coding for Penetration Testers - Building Better Tools**, Syngress, 2012.
- BISHOP, M. **Computer security: art and science**. Boston: Addison Wesley, 2003.
- DA COSTA, Kelton Augusto Pontara. **Segurança em Redes de Computadores**, notas de aula (redes), 2013.
- ERICKSON, Jon. **Hacking: The Art Of Exploitation**, No Starch Press 2008.
- FLORENTINO, Adilson Aparecido. **IPv6 na prática**, Coleção Academy 2012.
- HAUSER, Van. **Attacking the IPv6 protocol suite**, THC 2008.
- KENNEDY, David; O'GORMAN, Jim; KEARNS, Devon; AHARONI, Mati. **Metasploit: The Penetration Tester's Guide**, No Starch Press 2011.
- KUROSE, James F.; ROSS, Keith W. . **Redes de computadores e a Internet**, uma abordagem top-down. 3ª edição, Pearson Addison Wesley 2006.
- McCUMBER. **Information Systems Security: A comprehensive Model**. Proceedings of the 14th National Computer security Conference. Baltimore, 1991.
- NESTLER, Vincent; CONKLIN, Wm. Arthur; WHITE, Gregory; HIRSCH, Matthew. **Principles of Computer Security: CompTIA Security+ and beyond Lab Manual**, Mc Graw Hill 2011.
- OLIVEIRA, Ronielton Resende. **Criptografia simétrica e assimétrica: os principais algoritmos de cifragem**, disponível em: <http://www.ronielton.eti.br/publicacoes/artigorevistasegurancadigital2012.pdf>. (acesso em 23/11/2014).
- PILIHANTO, Atik. **A Complete Guide on IPv6 Attack and Defense**, SANS Institute 2011.
- SCARFONE, Karen; MELL, Peter. **Guide to Intrusion Detection and Prevention Systems (IDPS)**, NIST 2007.
- TAMEGA, Flavio. **Hacker Inside - Top Secret**, Terra, 2003.
- THC, Disponível em: <https://www.thc.org/thc-ipv6> (acesso em 23/05/2014).
- ULBRICH, Henrique Cesar; DELLA VALLE, James. **Universidade Hacker**, Digerati Books 2004.

US-CERT. **Security Tip(ST04-015)** , disponível em: <https://www.us-cert.gov/ncas/tips/ST04-015>. (acesso em 27/01/2015).

MACONACHY, W.V; SCHOU. C; RAGSDALE. D; WELCH. D. **A model for information Assurance: an Integrated Approach**. Proceeding of the 2001 IEEE Workshop on Information Assurance and Security. West Point, 2001.