SIMULAÇÃO DE ATAQUE DoS: COMPORTAMENTO DOS PROTOCOLOS DE INTERNET EM PILHA DUPLA

DoS ATTACK SIMULATION: BEHAVIOR OF DUAL STACK INTERNET PROTOCOLS

Henrique Rodrigues Nunes
Fatec Americana
henrique.nunes3@fatec.sp.gov.br

Vinícius Coquette de Carvalho
Fatec Americana
vinicius.carvalho27@fatec.sp.gov.br

Henri Alves de Godoy
Fatec Americana
henri.godoy@fatec.sp.gov.br

Resumo

Este artigo discorre sobre o comportamento dos protocolos de Internet nos servidores em pilha dupla (*dual-stack*), ao serem sobrecarregados com inúmeras solicitações simultâneas, em observância ao impacto em seus respectivos protocolos IPv4 e IPv6. O objetivo desta pesquisa é corroborar com o conhecimento na área de tecnologia a respeito de ataques de negação de serviço (*denied of service*) em servidores com pilha dupla. Visa contribuir para o conhecimento especialmente em ataques de negação de serviço em tais servidores. A metodologia de pesquisa é qualitativa e de natureza aplicada com pesquisas bibliográficas em artigos e publicações acadêmicas, baseadas no tema e pesquisas documentais, coletando informações na literatura e websites de busca academicos, a fim de configurar o ambiente de testes. Como resultado, pelo menos um dos endereços IP atribuído a interface não foi afetado, mantendo assim, a estabilidade e continuidade dos serviços.

Palavras-chave: estabilidade; vulnerabilidade; protocolos; IPv4; IPv6.

Abstract

This paper discusses the behavior of Internet protocols on dual-stack servers when overloaded with numerous simultaneous requests, observing the impact on their respective IPv4 and IPv6 protocols. The objective of this research is to corroborate the knowledge in the technology area regarding denial of service attacks on dual-stack servers. It aims to contribute to the knowledge, especially on denial of service attacks on such servers. The research methodology is qualitative and of an applied nature with bibliographic research in academic articles and publications, based on the theme and documentary research, collecting information in the literature and academic search websites, to configure the test environment. As a result, at least one of the IP addresses assigned to the interface was not affected, thus maintaining the stability and continuity of services.

Keywords*: stability; vulnerability; protocols; IPv4; IPv6*

1. Introdução

Um dos grandes desafios encontrados no âmbito da tecnologia é a estabilidade, ainda mais com o crescimento dos usuários e dispositivos que consequentemente ocasiona o aumento dos Protocolos de Internet (*Internet Protocol*) na rede.

O avanço contínuo das tecnologias de comunicação, somado ao aumento da quantidade de dispositivos conectados à Internet, apresentou novas barreiras para o Protocolo de Internet versão 4 (IPv4). Criado nos estágios iniciais da era digital, o IPv4 logo se deparou com o iminente esgotamento de cerca de 4,2 bilhões de endereços exclusivos. Na virada do milênio, ano 2000, o esgotamento dos blocos de endereços IPv4 disponíveis já era uma preocupação evidente.

O crescimento de dispositivos conectados, incluindo computadores, dispositivos móveis e Internet das Coisas (IoT), exacerbou a inadequação do IPv4 para suportar a crescente demanda por endereços IP únicos.

Durante esse período de transição, a porcentagem de tráfego utilizando IPv6 aumentou gradualmente, refletindo o reconhecimento da necessidade de uma infraestrutura de Internet mais expansível. Empresas líderes de tecnologia passaram a habilitar suporte IPv6 em seus serviços, contribuindo para a aceitação e implementação generalizada do novo protocolo. Essas medidas foram essenciais para garantir a continuidade e o crescimento saudável da conectividade global em face das limitações iminentes do IPv4.

O IPv6 surgiu para resolver a escassez de endereços. No entanto, uma das mudanças necessária de mentalidade aconteceu com a utilização e o não bloqueio do protocolo *Internet Control Message Protocol Version 6 (ICMPv6)*, protocolo essencial no IPv6, utilizado para comunicação entre dispositivos na Internet, incluindo funções como diagnósticos de rede e configuração automática de endereços, primordial para o funcionamento de recursos. Isso aumentou as possibilidades de ataques de rede, incluindo ataques de Negação de Serviço (DoS), um tipo de ataque que visa sobrecarregar um sistema, tornando-o inacessível para usuários legítimos, no qual será abordado ao longo do artigo.

Tendo em vista que o IPv4 ainda é bastante utilizado e o IPv6 se tornou funcional, criou-se a possibilidade de utilizar serviços em pilha dupla, podendo assim ter dois IP funcionais em apenas uma interface de rede de um servidor.

Questiona-se, então, como pergunta do problema de pesquisa: caso um servidor em pilha dupla recebesse um ataque DoS de em um de seus endereços, teria impacto geral ou somente no endereço alvo?

O objetivo desta pesquisa é analisar o funcionamento de uma rede com um servidor Web em pilha dupla ao ser sobrecarregado em um de seus endereços IP. Será analisado a negação de serviço no IPv4, a fim de comparar o impacto no acesso do serviço Web em IPv6.

A justificativa da relevância da pesquisa é corroborar com o conhecimento dos ataques DoS em IPv4 e IPv6. Dessa forma, comprovar se um servidor em pilha dupla teria alguma vantagem nessas investidas ou se aumentariam as vulnerabilidades na rede.

Nesse contexto, há que se destacar o uso protocolo *Transmission Control Protocol (TCP)* para encaminhar uma quantidade enorme de solicitações ao servidor de destino, e o protocolo *Internet Control Message Protocol (ICMP)*, o qual tem a função de enviar diversos pacotes, para o dispositivo de destino e aguardar uma resposta, geralmente utilizado para verificar se uma máquina remota está ativa e disponível. Lembrando que em alguns casos o ICMP é desativado no servidor, para evitar ataques que possuem a função de esgotar recursos e tornar um serviço inacessível para usuários legítimos. Como resultado da exploração proporcionada pelo ataque de DoS, os usuários não conseguem acessar a aplicação, causando prejuízos financeiros ou perda de reputação do alvo afetado.

As áreas do conhecimento, no âmbito de Segurança da Informação que contribuíram para a realização desta pesquisa, foram: configurações de servidores e funcionamento dos protocolos de rede, facilitando o entendimento no tema apresentado.

O artigo está organizado da seguinte maneira: após esta Introdução, o Referencial Teórico, para apresentar os principais conceitos, teorias, modelos e pesquisas desenvolvidas sobre o assunto em questão; posteriormente, em Materiais e Métodos, há uma descrição detalhada e sistemática dos métodos realizados para a pesquisa. Em seguida, os Resultados e Discussões apresentarão objetivamente os resultados de todos os testes e, por fim, as Considerações Finais, que apresentarão uma síntese dos principais resultados e conclusões.

2. Referencial Teórico

O referencial teórico deste estudo abrange dois pilares essenciais: os distintos tipos de ataques de negação de serviço e os protocolos de rede que desempenham um papel crítico no tema apresentado. O ambiente digital atual enfrenta constantes desafios de segurança, e a compreensão aprofundada desses elementos é crucial para a integridade da rede.

2.1. Ataque DoS

Os ataques de negação de serviço (DoS), são um problema muito sério na Internet, cujo impacto é demonstrado na literatura de rede de computadores.

O principal objetivo de um DoS é a interrupção de serviços ao tentar limitar o acesso a uma máquina ou serviço. Esses ataques atingem seu objetivo enviando à vítima uma rajada de pacotes que sobrecarregam sua capacidade de rede ou processamento, negando acesso a seus clientes regulares. Segundo os autores, a duração desses ataques pode variar de alguns segundos há vários dias e as perdas para os provedores de serviços podem ser significativas.

Embora existam várias técnicas de defesa baseadas em inteligência artificial, computação de alto desempenho ou sistemas de prevenção de intrusões para se defender destes ataques. O DoS mantém-se com ataques em larga escala direcionados a sites de alto perfil na Internet (Douligeris, Mitrokotsa, 2004, p. 190).

2.2. SYN Flood

Os ataques de SYN-flooding são estratégias maliciosas que exploram uma vulnerabilidade no protocolo TCP, sobrecarregando um servidor com solicitações de origem de conexão falsa. Eles se aproveitam do mecanismo de *handshake* de três etapas do TCP, gerando um grande número de solicitações de conexão, mas não concluindo o processo, deixando conexões “meio abertas”. Essa técnica pode esgotar os recursos da rede, impedindo que conexões legítimas sejam estabelecidas.

O ataque de SYN-flooding é uma forma de negação de serviço (DoS) que pode causar sérios danos aos sistemas e à disponibilidade dos serviços online. Ao inundar um servidor com solicitações SYN, os atacantes podem sobrecarregar a capacidade do servidor de processar novas conexões legítimas, levando à queda do serviço para usuários legítimos.

Detectar esse tipo de anomalia na rede é um desafio complexo, pois depende da análise do comportamento normal do tráfego da rede e da identificação de padrões anômalos.

As defesas contra-ataques de SYN-flooding incluem *firewalls*, filtros de pacotes e técnicas de mitigação de ataques DoS para ajudar a proteger os sistemas contra essas investidas maliciosas (MANNA e AMPHAWAN, 2021, p. 101).

2.3. IPv4 e IPv6

O IPv4, sendo o protocolo mais antigo e amplamente empregado na atualidade, possui um endereço de 32 bits que permite cerca de 4,2 bilhões de endereços. Contudo, desde 2011, o IPv4 está esgotado, dificultando a obtenção de endereços para novos usuários da Internet. O IPv6, como a versão mais recente do Protocolo Internet, foi desenvolvido para atender às crescentes demandas dos usuários, apresentando um endereço de 128 bits que suporta aproximadamente 3,4 undecilhão de endereços. Além disso, o IPv6 introduz outras alterações em comparação com o IPv4, as quais serão abordadas posteriormente. No entanto, surgem preocupações quanto à implementação e segurança do IPv6. Alguns dispositivos de segurança ainda não são compatíveis com o IPv6, e outros que oferecem suporte podem não estar devidamente configurados pelos administradores. Como resultado, determinados *firewalls* e sistemas de detecção e prevenção de intrusões podem identificar tráfego malicioso IPv4, mas um atacante pode potencialmente contornar esses mecanismos enviando tráfego malicioso IPv6 (PILIHANTO, 2012, p.3).

2.4. O Modelo TCP/IP

O TCP é um protocolo da camada de transporte fundamental, conhecido por sua capacidade de transferir dados de forma confiável, garantindo que as informações enviadas pelo remetente sejam recebidas pelo destinatário. É por meio do TCP que as conexões de Internet são viabilizadas.

A transferência de dados pelo TCP é realizada mediante processo conhecido como *three-way handshake*. Esse processo envolve a troca de mensagens entre a origem e o destino antes que os dados sejam transmitidos com segurança. (Moreno, 2015, p. 103).

O protocolo TCP usa um procedimento chamado de aperto de mão em três vias para iniciar uma conexão. Antes de o cliente se conectar, o servidor precisa primeiro abrir e escutar sua própria porta, chamado de abertura passiva. Depois disso, o cliente pode iniciar uma abertura ativa. O aperto de mão em três vias ocorre da seguinte maneira:

O cliente envia um segmento SYN para o servidor, estabelecendo assim a abertura ativa, resposta, o servidor envia um SYN-ACK de volta ao cliente estabelecendo assim a abertura ativa e finalmente, o cliente envia um ACK de volta ao servidor concluindo a comunicação. Isso permite que eles falem um com o outro em duas direções ao mesmo tempo, como se fosse um bate-papo onde ambos podem falar e ouvir ao mesmo tempo (FRAGA, 2019, p. 208).

2.5. Protocolo HTTP

O HTTP (Protocolo de Transferência de Hipertexto) é o protocolo fundamental da Web, definido inicialmente pelas RFC 1945 e 2616. Já obsoletas, hoje há um conjunto de RFC que descrevem o HTTP como: RFC 7230, RFC 7231, RFC 7232, RFC 7233, RFC 7234, RFC 7235. Ele opera entre clientes e servidores, permitindo a troca de mensagens HTTP. As páginas da Web são compostas por objetos, como arquivos HTML, imagens, *applets* e vídeos, cada um acessado por um URL. O HTTP define como os clientes solicitam objetos aos servidores e como esses objetos são transmitidos. O HTTP usa o TCP como protocolo de transporte. Quando um usuário clica em um link em um página Web, o navegador envia mensagens de requisição HTTP para o servidor, que responde com mensagens de resposta contendo os objetos. O HTTP é um protocolo sem estado, o que significa que os servidores não mantêm informações sobre os clientes. A Web utiliza uma arquitetura cliente-servidor, onde os servidores estão sempre disponíveis para atender às solicitações de vários navegadores (KUROSE e ROSS, 2013, p. 72).

3. Materiais e Métodos

Neste estudo, realizou-se uma pesquisa qualitativa, havendo uma pesquisa bibliográfica sobre o tema de DoS aplicados aos protocolos de Internet IPv4 e IPv6, cujas principais obras referenciadas neste contexto são: “Técnicas de Invasão: Aprenda as técnicas usadas por hackers em invasões reais”, escrito por Bruno Fraga, que trouxe um entendimento da comunicação entre cliente e servidor. O artigo “*DoS attacks and defense mechanisms*”, dos autores Christos Douligeris e Aikaterini Mitrokotsa, esclarecendo o funcionamento e o conceito de um ataque DoS. A fim de ter um maior entendimento do IPv6 e suas vulnerabilidades, foi aprofundada a análise do e-book “*A Complete Guide on IPv6 Attack and Defense*”, criado pelo especialista Atik Pilihanto. Para a execução prática, foi utilizado alguns dos conhecimentos adquiridos no livro “Introdução ao Pentest”, conduzido por Daniel

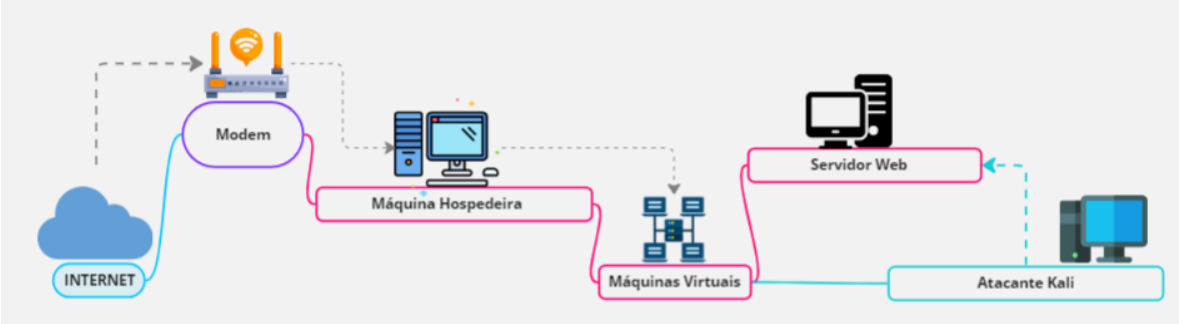
Moreno. Com o intuito de aprofundar os estudos em protocolos de rede e IPv4, a obra “Redes de Computadores e a Internet: Uma Abordagem Top-Down”, dos autores Jim Kurose e Keith Ross, foi consultada.

As fontes de obtenção dos materiais de pesquisas foram obtidas por meio de livros; consulta a artigos acadêmicos nos sites do Google Acadêmico e “*SANS Institute*”, bem como arquivos disponibilizados pelo orientador deste artigo.

A representação foi realizada atacando apenas o protocolo IPv4, pois a maioria dos ataques são feitos neste protocolo, tendo em vista, a escassez de ferramentas de ataques em IPv6. Foi realizado um teste para verificar se um servidor em pilha dupla seria a solução, com isso, será analisado se o ataque afetará o IPv6 e se o serviço ainda estará disponível por este endereço.

Todo o ambiente foi configurado em uma rede interna, pois o provedor de Internet utilizados nos testes, bloqueia o acesso externo ao IPv6. Portanto, o acesso às páginas Web é permitido para as máquinas que estiverem na rede, desta forma será possível simular a conexão entre cliente e servidor.

Figura 1: Cenário de Ataque



Fonte: Autoria própria (2023)

Conforme exemplificado na Figura 1, simulou-se o ataque em uma rede *Local Area Network (LAN)*, na qual havia um modem, como porta de entrada/saída da Internet, conectado a uma máquina hospedeira que alojava máquinas virtuais. Essas máquinas virtuais são compostas por um servidor Web e uma máquina atacante.

3.1. Máquina Hospedeira

Na máquina hospedeira, o Windows 11 (Microsoft Corporation, 2021), se encontra como sistema operacional, onde foi instalado e configurado o *PRTG Network Monitor*

(Paessler AG, 2023), serviço cujo objetivo é monitorar as interfaces de rede do servidor, tempo de carregamento da página Web e a disponibilidade das máquinas.

Para configuração do monitoramento das interfaces de rede, foi configurado o protocolo *Simple Network Management Protocol (SNMP)*, utilizado para monitorar e gerenciar dispositivos de rede. Ele permite a coleta de informações sobre a condição e o desempenho dos dispositivos, bem como, modificarem suas configurações.

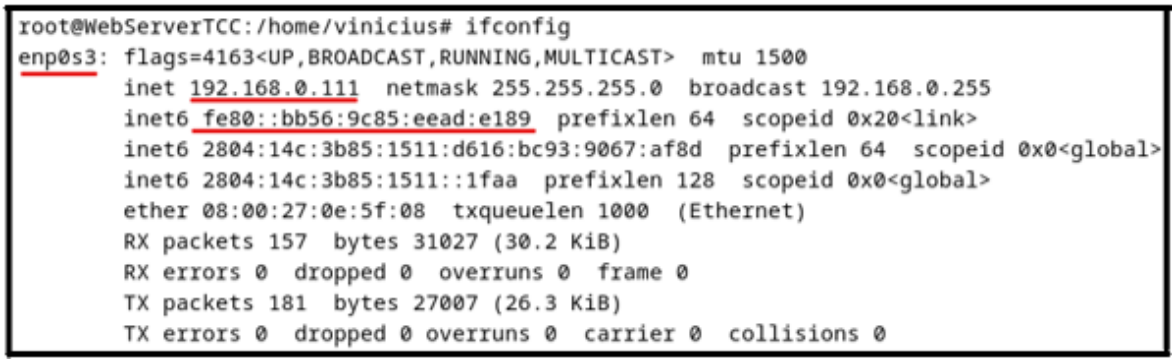
3.2. Servidor Web

No servidor Web, foi utilizado o Debian (Debian Project, 2023), como sistema operacional, tendo como serviço Web, o Apache 2.4.58 (Apache Software Foundation, 2023). A interface de rede do servidor foi configurada como pilha dupla.

Para monitoramento de pacotes e tráfego de entrada, foi instalado o Wireshark (Wireshark, 2023).

Foi estabelecido dois cenários de testes. No primeiro, a situação é definida por um servidor Web configurado em pilha dupla, utilizando apenas uma interface de rede "enp0s3", conforme Figura 2.

Figura 2: Interface de Rede do Servidor Web – Cenário 1



Fonte: Autoria própria (2023)

Neste cenário, a interface recebeu como endereços locais o IPv4: 192.168.0.111 e o IPv6: fe80::bb56:9c85:eead:e189.

No segundo cenário de testes, o servidor Web foi configurado com duas interfaces de rede em pilha dupla, a já existente "enp0s3", configurada somente com IPv4 e a nova "enp0s8", configurada apenas com IPv6, conforme Figura 3.

Figura 3: Interfaces de Rede do Servidor Web – Cenário 2

```
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.111  netmask 255.255.255.0  broadcast 192.168.0.255
        ether 08:00:27:0e:5f:08  txqueuelen 1000  (Ethernet)
        RX packets 65  bytes 12500 (12.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 63  bytes 8505 (8.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 2804:14c:3b85:1511:6016:ef17:33e:a3a3  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::67d7:9743:b2be:7a3b  prefixlen 64  scopeid 0x20<link>
        inet6 2804:14c:3b85:1511::19e3  prefixlen 128  scopeid 0x0<global>
        ether 08:00:27:f8:32:63  txqueuelen 1000  (Ethernet)
        RX packets 84  bytes 18985 (18.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 88  bytes 13289 (12.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Fonte: Autoria própria (2023)

Neste cenário, o IPv4, manteve o endereço local: 192.168.0.111 e o IPv6, recebeu o endereço local: fe80::67d7:9743:b2be:7a3b.

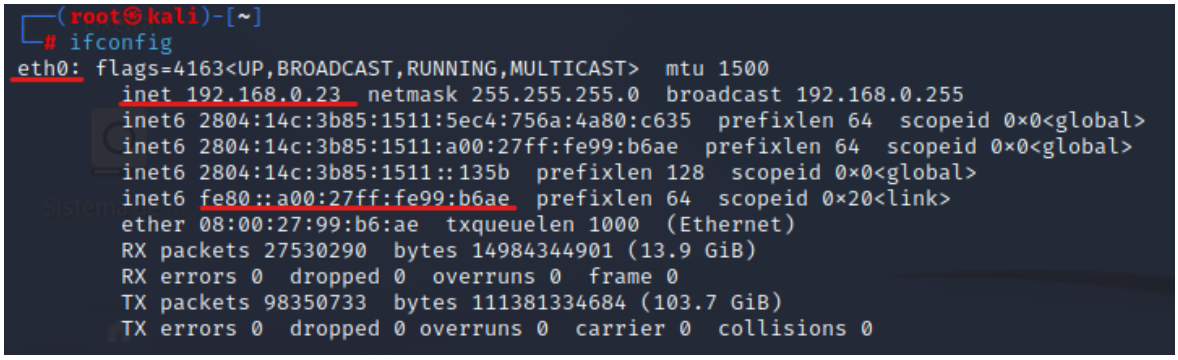
3.3. Máquina Atacante

Os ataques foram realizados utilizando o sistema operacional, Kali Linux (Offensive Security, 2023). O Kali é uma distribuição GNU/Linux baseada no Debian, completo para uso em ataques de rede, com uma ampla gama de ferramentas e recursos para realizar uma variedade de tarefas.

Como ferramenta de ataque DoS, foi utilizado o Hping3, um software padrão do Kali Linux, para enviar pacotes IP com o sinalizador SYN ativo para um destino. O sinalizador SYN é usado para iniciar uma conexão TCP, mas no caso do Hping, o atacante não envia o segundo pacote TCP necessário para completar a conexão. Isso faz com que o destino mantenha recursos abertos para a conexão, o que pode levar ao esgotamento de recursos e a indisponibilidade do serviço.

A interface de rede da máquina atacante, foi configurada como “eth0”, recebendo os endereços locais, IPv4: 192.168.0.23 e IPv6: fe80::a00:27ff:fe99:b6ae, conforme ilustrado na Figura 4.

Figura 4: Interface de Rede da Máquina Atacante



Fonte: Autoria própria (2023)

4. Resultados e Discussões

A fim de demonstrar a efetividade de um ataque DoS, foi executado, de primeiro momento, um ataque de alta intensidade. Já, nos cenários 1 e 2, o ataque passou a ser de baixa intensidade, portanto, não causou a indisponibilidade do servidor, apenas o deixou sobrecarregado, para que o comportamento dos protocolos fosse monitorado e analisado. Em seguida, para melhor entendimento dos protocolos na rede, o monitoramento dos pacotes foi executado. Também, um breve detalhamento de prevenções contra ataques de negação de serviço, foi discorrido.

4.1. Demonstração de Ataque DoS

Antes dos ataques, a página do servidor Web foi acessada a partir da máquina hospedeira, utilizando os endereçamentos IPv4 e IPv6. Foi confirmado sucesso nos acessos, como ilustrado nas Figuras 5 e 6.

Figura 5: Página Web em Funcionamento

Fonte: Autoria própria (2023)

Figura 6: Página Web em Funcionamento

Fonte: Autoria própria (2023)

Com o ambiente devidamente configurado, a máquina virtual atacante executou um ataque DoS, com a ferramenta Hping, enviando diversos pacotes e requisições SYN/TCP contra o endereço IPv4 192.168.0.111, sobrecarregando-o.

A Figura 7, mostra o comando utilizado, onde consistiu em encaminhar solicitações ao endereço IPv4, na porta 80, no menor tempo possível, utilizando o comando '`—flood`'; para sobrecarregar os servidores.

Figura 7: Comando de Ataque

```
┌──(root㉿kali)-[~]
└─# hping3 -S --flood 192.168.0.111 -p 80
HPING 192.168.0.111 (eth0 192.168.0.111): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Fonte: Autoria própria (2023)

Como mostra a Figura 8, o ataque resultou no aumento do tempo de carregamento das páginas Web, no servidor. Após o ataque, o tempo no carregamento da página, atingiu picos de 8 segundos, logo depois, houve a queda do serviço, como mostra a frase de erro, na coluna "Tempo de Carregamento".

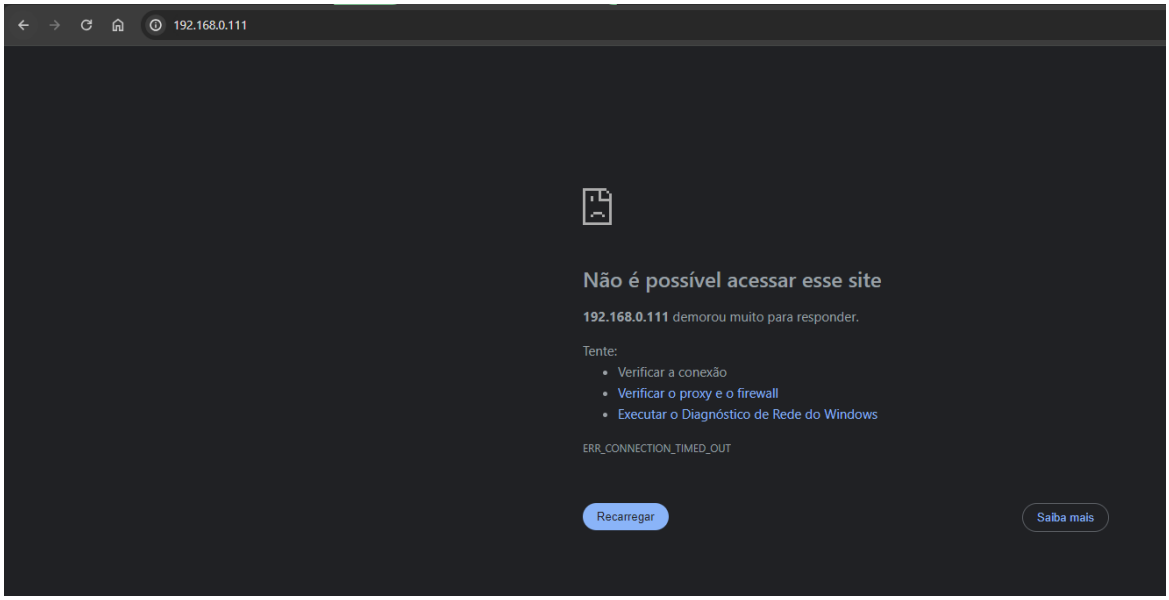
Figura 8: Tempo de Carregamento da Página Web

Data e hora	Tempo de carregamento	Tempo de inoperância	Cobertura
01/11/2023 16:22:41	Erro	Erro	100 %
01/11/2023 16:22:19	Erro	Erro	100 %
01/11/2023 16:21:36	8.118 ms	0 %	100 %

Fonte: Autoria própria (2023)

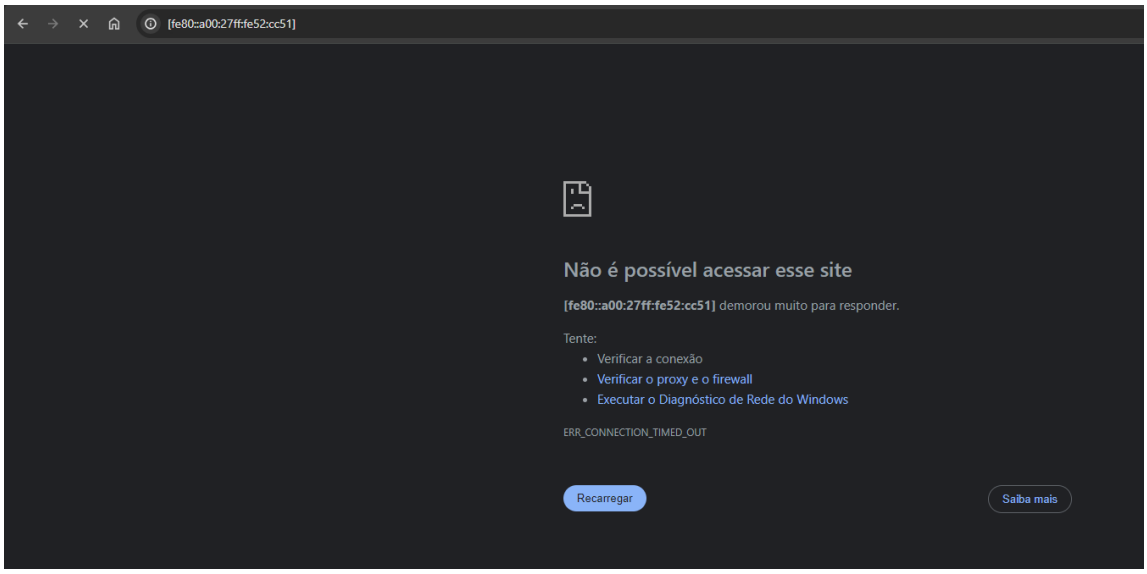
O ataque resultou na indisponibilidade do serviço Web, nos dois servidores, tanto no protocolo IPv4 quanto no IPv6, conforme mostra a Figura 9 e 10, enquanto acessado pela máquina hospedeira. Este é o impacto causado por um ataque DoS.

Figura 9: Indisponibilidade da Página no IPv4



Fonte: Autoria própria (2023)

Figura 10: Indisponibilidade da Página no IPv6



Fonte: Autoria própria (2023)

4.2. Cenário 1: Ataque com Uma Interface de Rede

Neste cenário, um ataque DoS de baixa intensidade foi executado no IPv4 do servidor em pilha dupla, configurado com apenas uma interface de rede, suportando IPv4 e IPv6; a fim de capturar o impacto nos dois protocolos, sem causar a indisponibilidade da rede, causando apenas lentidão, podendo assim, analisar o comportamento de ambos ao receberem pacotes SYN/TCP.

Ao iniciar o ataque contra o servidor, pode ser observado um aumento no tempo de carregamento da página, acessando pelo IPv4, chegando em picos de quase 31 segundos, como demonstrado na Figura 11.

Figura 11: Tempo de Carregamento da Página Web no IPv4 – Cenário 1

Data e hora	Tempo de carregamento	Tempo de inoperância	Cobertura
15/11/2023 18:44:06	16.480 ms	0 %	100 %
15/11/2023 18:43:21	31.078 ms	0 %	100 %

Fonte: Autoria própria (2023)

Acessando pelo IPv6, o mesmo comportamento do IPv4 pode ser observado, atingindo picos de 28 segundos, como mostrado na Figura 12.

Figura 12: Tempo de Carregamento da Página Web no IPv6 – Cenário 1

Data e hora	Tempo de carregamento	Tempo de inoperância	Cobertura
15/11/2023 18:44:06	13.481 ms	0 %	100 %
15/11/2023 18:43:42	19.267 ms	0 %	100 %
15/11/2023 18:43:21	28.081 ms	0 %	100 %

Fonte: Autoria própria (2023)

4.3. Cenário 2: Ataque com Duas Interfaces de Rede

No cenário 2, foi executado outro ataque DoS de baixa intensidade, porém, com o servidor em pilha dupla, configurado com duas interfaces de rede, uma utilizando somente IPv4 e outra IPv6.

Desta forma, foi analisado o comportamento dos dois protocolos, enquanto o servidor foi sobrecarregado em apenas um endereço: o IPv4, sem “derrubar” o serviço.

Após início do ataque, pode ser observado, novamente, um aumento no tempo de carregamento da página quando acessado pelo IPv4. Picos de 39 segundos podem ser analisados, conforme Figura 13.

Figura 13: Tempo de Carregamento da Página Web no IPv4 – Cenário 2

Data e hora	Tempo de carregamento	Tempo de inoperância	Cobertura
15/11/2023 21:34:29	39.036 ms	0 %	100 %
15/11/2023 21:33:45	25.708 ms	0 %	100 %

Fonte: Autoria própria (2023)

No momento do ataque, ao realizar o acesso na página pelo IPv6, não houve tal lentidão, atingindo picos de, somente, 3 milissegundos, conforme Figura 14. Comportamento contrário comparado ao cenário 1 em que os dois protocolos estavam juntos na única interface de rede do servidor.

Figura 14: Tempo de Carregamento da Página Web no IPv6 – Cenário 2

Data e hora	Tempo de carregamento	Tempo de inoperância	Cobertura
15/11/2023 21:34:29	2 ms	0 %	100 %
15/11/2023 21:33:45	3 ms	0 %	100 %

Fonte: Autoria própria (2023)

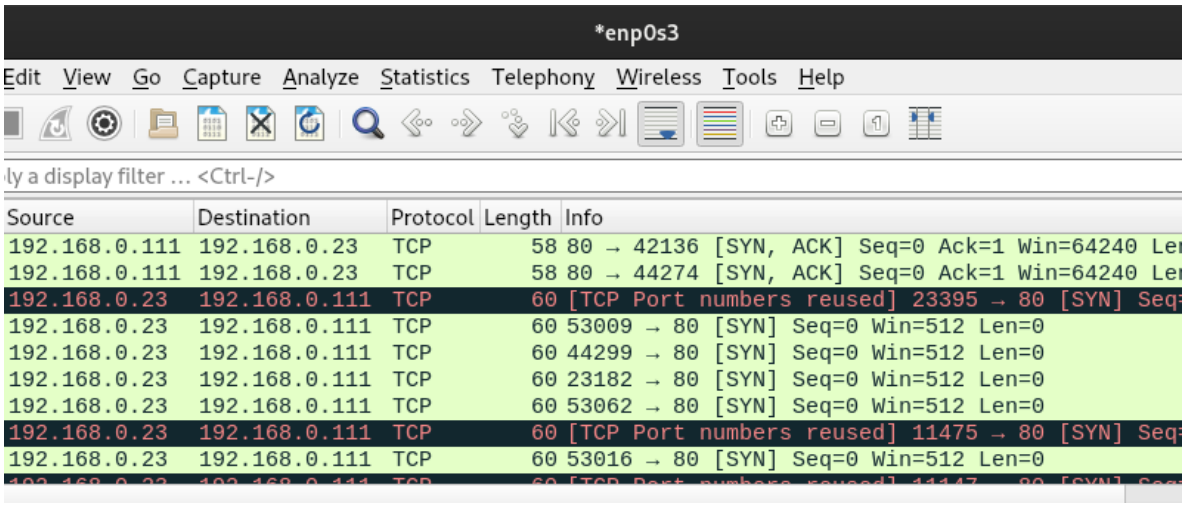
4.4. Monitoramento de Pacotes

A fim de monitorar o tráfego de entrada do servidor Web, foi obtido algumas amostras das análises de pacotes, utilizando o Wireshark.

No início dos ataques, pode ser observado na Figura 15 a inundação de pacotes TCP ao servidor, tendo como origem o endereço IP: 192.168.0.23.

Também, na coluna *"Source"* o servidor Web, com o IP: 192.168.0.111, recebendo os pacotes TCP enviados pelo atacante, IP: 192.168.1.23, na coluna "*Destination*". Na coluna "*Info*" pode ser visualizado as solicitações SYN, ACK ao servidor.

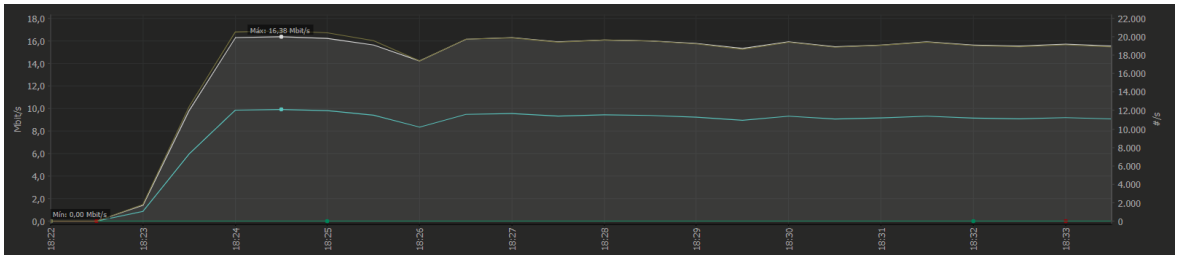
Figura 15: Tráfego de Pacotes - TCP



Fonte: Autoria própria (2023)

O tráfego de entrada do servidor Web, no início do ataque, pode ser visualizado no gráfico a seguir. Observe na Figura 16, o crescimento do tráfego no servidor alvo, um total de 16,38 Mbit/s.

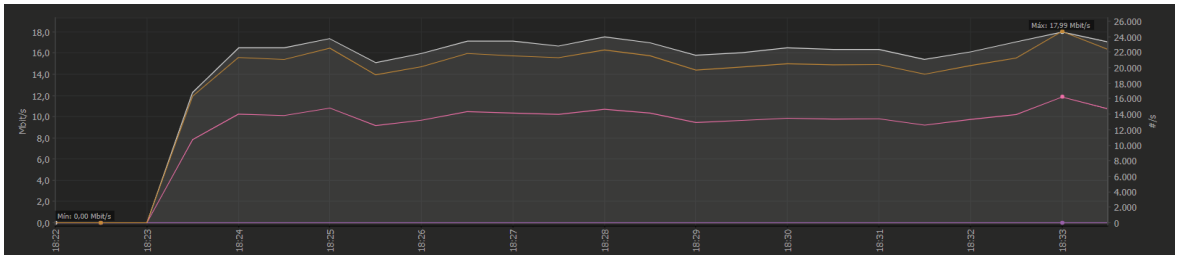
Figura 16: Tráfego de Entrada do Servidor Web



Fonte: Autoria própria (2023)

A análise do tráfego de saída da máquina atacante, no início do ataque, pode ser visualizada no gráfico a seguir. Na Figura 17, o crescimento do tráfego de saída, um total de 17,99 Mbit/s, pode ser visualizado.

Figura 17: Tráfego de Saída da Máquina Atacante



Fonte: Autoria própria (2023)

Em resumo, o monitoramento do tráfego, realizado via Wireshark, e PRTG, destacou a inundação de pacotes TCP e solicitações SYN-ACK no início do ataque.

4.5. Prevenção Contra DoS

A segurança em um servidor de pilha dupla, que suporta tanto o IPv4 quanto o IPv6, é bastante complexa, os bloqueios no *firewall* precisariam ser criados separadamente, considerando as diferenças e particularidades entre o IPv4 e IPv6. No entanto, isso é necessário para evitar ataques DoS. A limitação de banda também evitaria este tipo de ataque, já que você poderia limitar a quantidade de banda de um cliente. Desta forma, um ataque volumétrico não funcionaria.

Por fim, a segurança em um servidor de pilha dupla é bastante complexa e exigirá um alto nível de restrições, autenticações e autorizações, a fim de garantir a disponibilidade e estabilidade dos serviços.

5. Considerações Finais

As simulações realizadas neste artigo permitem concluir que em um cenário onde o ataque seja de baixa escala, a melhor escolha para um servidor em pilha dupla é configurá-lo com duas interfaces de rede, separando assim o IPv4 do IPv6. Dessa forma, caso uma de suas interfaces seja sobrecarregada, por exemplo, pelo IPv4, não terá tanto impacto no IPv6, causando mais estabilidade. No entanto, se for realizado um ataque volumétrico de larga escala direcionado à rede, a configuração não fará diferença.

Visto que o IPv6 ainda se encontra numa fase de transição, a escassez de ferramentas de ataques com suporte a IPv6 ainda é grande, quando comparado ao IPv4. Assim como, a alta quantidades de dispositivos conectados unicamente em IPv4. Isso resulta no aumento de ataques na versão 4 do protocolo, transformando-o em um alvo principal.

Os testes mostraram que um servidor em pilha dupla, pode trazer algumas vantagens em relação a ataques DoS, pois em determinados ataques, como o citado neste artigo, utilizando a configuração correta, poderá ser evitado instabilidades no protocolo de Internet e garantir a estabilidade da aplicação, fazendo com que continue funcionando em um de seus endereços IPs.

Referências

APACHE SOFTWARE FOUNDATION. Versão 2.4.51. Apache: HTTP Server Project. Disponível em: https://httpd.apache.org/. Acesso em: 15 jul. 2023.

DANTAS, Yuri Gil. Estratégias para tratamento de ataques de negação de serviços na camada de aplicação em redes IP. 78f. Dissertação (Mestrado em Ciência da Computação), Centro de Informática do Programa de Pós-Graduação em Informática, da Universidade Federal da Paraíba, João Pessoa, 2015. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/tede/7841/2/arquivototal.pdf. Acesso em 28 nov. 2023.

DEBIAN. Versão 11.1.0. Disponível em: https://www.debian.org/distrib/. Acesso em: 12 jul. 2023

DOULIGERIS, Christos; MITROKOTSA, Aikaterini. DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer Networks, 2004. Vol. 44, Issue 5, p. 643-666. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1389128603004250. Acesso em: 28 nov. 2023.

FRAGA, Bruno. Técnicas de Invasão: Aprenda as técnicas usadas por hackers em invasões reais. 1ª ed. São Paulo: Editora Labrador, 2019.

HPING3. Versão 21.4.70. Disponível em: https://github.com/antirez/hping. Acesso em: 15 jul. 2023.

KALI LINUX. Versão 2021.3. Disponível em: *https://www.kali.org/downloads/*. Acesso em: 12 jul. 2023.

KUROSE, James F.; ROSS, Keith W. Redes de Computadores e a Internet: Uma Abordagem Top-Down. 6ª ed. São Paulo: Pearson Education, 2013, p. 72.

MANNA, Mehdi Ebady; AMPHAWAN, Angela. Review of SYN-flooding attack detection mechanisms. In: 2021 IEEE 18th International Conference on Advanced Communication Technology (ICACT), 2021, Jeju, South Korea. Proceedings. Piscataway, NJ: IEEE, 2021. p. 101-106. Disponível em: https://arxiv.org/ftp/arxiv/papers/1202/1202.1761.pdf. Acesso em: 20 jul. 2023.

MICROSOFT CORPORATION. Microsoft Windows 11. Redmond, WA: Microsoft. Disponível em: https://www.microsoft.com/pt-br/windows/. Acesso em: 15 jul. 2023.

MORENO, Daniel. Introdução ao Pentest. São Paulo: Novatec 2015

PILIHANTO, Atik. A Complete Guide on IPv6 Attack and Defense. 1ª ed. SANS Institute, 2012. Disponível em: https://sansorg.egnyte.com/dl/9f6wOPsY7s. Acesso em: 22 jul. 2023.

PRTG NETWORK MONITOR. Versão 21.4.70.1629. Disponível em: *https://www.paessler.com/prtg/download*. Acesso em: 15 jul. 2023.

WIRESHARK. Versão 3.6.5. Disponível em: https://www.wireshark.org/download.html. Acesso em: 15 jul. 2023.