Mitigação de ataques DoS e DDoS utilizando Nginx

Bruno Haesbaert Pippi[1], Alessandro Andre Mainardi de Oliveira[1], Reiner Franthesco Perozzo[1] (Em memória)

[1]Ciência da Computação – Universidade Franciscana (UFN)
Cep – 97.010-030 – Santa Maria – RS – Brasil

bruno.haesbaert.p@gmail.com, alessandroandre@ufn.edu.br

Abstract. *Due to technological advances and the growing search for technology in this work, penetration tests, protection and monitoring of server attacks will be carried out. In a virtual machine (Ubuntu 20.04), a reverse-proxy server will be implemented using the Nginx Plus tool to camouflage the local IP of a given server, together with traffic control and bandwidth restriction to block possible DoS attacks and prevent larger attacks like DDoS.*

Resumo. *Devido ao avanço tecnológico e a crescente busca por tecnologia neste trabalho serão elaborados testes de invasão, proteção e monitoramento de ataques a servidores. Em uma máquina virtual, será implementado um servidor de proxy-reverso utilizando a ferramenta Nginx Plus para a camuflagem de IP local de um determinado servidor, juntamente o controle de tráfego e restrição de largura de banda para bloquear possíveis ataques DoS e prevenir ataques maiores como o DDoS.*

1.Introdução

O avanço da tecnologia muda com velocidade, promovendo a evolução e a flexibilidade do cotidiano dos seres humanos. Muitas pessoas não conseguem acompanhar a mudança de tanta tecnologia como deveriam, ficando assim expostas a diversas ameaças virtuais. Uma dessas ameaças é o ataque de negação de serviço (DoS), utilizado principalmente, em alvos como bancos, prefeituras e empresas de tecnologia com a finalidade de interromper seus serviços prestados a seus clientes e colocar em risco seus dados. Há também outro mecanismo de ataque mais eficaz que o DoS que é chamado de DDoS e é utilizado com o mesmo objetivo do DoS, porém, em maior escala causando assim maiores danos a companhia. Existem diversas formas de se proteger e de se prevenir contra esses tipos de ataques. A forma que será implementada neste trabalho é utilizando um proxy-reverso e balanceador de carga chamado Nginx.

Este projeto tem por objetivo demonstrar técnicas de proteção contra-ataques DoS e DDoS no nível de camada de aplicação e a comparação do comportamento de diferentes cenários alvos. Devido a proeminência da proteção contra-ataques cibernéticos, este trabalho mostrará a diferença entre alvos que estão expostos à internet e alvos teoricamente seguros, revelando a importância de se proteger de alguma maneira contra possíveis invasores.

Diante deste contexto este trabalho utilizará a metodologia *The Penetration Testing Execution Standard (PTS)* foi adotada para servir de base para a realização desta proposta, devido a amplitude e a importância, além de ser considerada um padrão a ser seguida para a realização de testes de invasão [PTES 2021].

2. Referencial Teórico

Esta seção trata exclusivamente da apresentação das ferramentas utilizadas neste trabalho, dentre eles; softwares, protocolos, mecanismos de ataque e camadas de redes. Procurando esclarecer a ideia inicial sobre o funcionamento de cada um deles, serão distribuídos em subseções para melhor entendimento e visualização.

2.1 Softwares

Nesta sessão serão mostrados os softwares utilizados neste trabalho.

2.1.1 Nginx: Nginx é um dos servidores web mais utilizado hoje em dia, devido as suas capacidades de balanceamento de carga HTTP e utilizar proxy reverso para protocolos de internet [Derek DeJonghe 2021]. Oficialmente lançado em outubro de 2004, o criador do software Igor Sysoev iniciou o projeto em 2002 como uma tentativa de solucionar o problema C10K (desafio de gerenciar dez mil conexões ao mesmo tempo). Nginx possui uma excelente capacidade de lidar com muitas conexões, e por esse motivo, vários sites de alto tráfego tem usado o serviço da NGINX, como Google, Netflix, Adoble, CloudFlare, WordPress entre outros [EVEO 2019].

2.1.2 Wireshark: A análise de rede é o processo de ouvir e analisar o tráfego da rede. A análise de rede oferece uma visão nas comunicações de rede para identificar problemas de desempenho, localizar violações de segurança, analisar aplicativos, comportamento e realizar o planejamento de capacidade. A análise de rede (também conhecida como "análise de protocolo") é um processo usado por profissionais de TI que são responsáveis pelo desempenho e segurança da rede [Chappell 2010].

2.2 Protocolos de comunicação

Nesta sessão serão mostrados os protocolos de comunicação utilizados neste trabalho.

2.2.1 IP: É um protocolo de comunicação usado entre todas as máquinas em rede para o encaminhamento dos dados encontrados na camada de rede. Esse protocolo funciona de forma semelhante ao CPF de uma pessoa física, permitindo que conexões entre dispositivos sejam identificadas a partir de uma sequência numérica. O *Internet Protocol* (IP) é utilizado para identificar dispositivos ou conexões e é chamado de IP *Address*, mas também existem outros como o TCP/IP que é utilizado para reconhecer a comunicação entre dois dispositivos distintos. [Boavida 2012].

2.2.2 HTTP: É um protocolo de transferência que possibilita que as pessoas que inserem a *Uniform Resource Locator* (URL) do seu site na Web possam ver os conteúdos e dados que nele existem. Esse sistema é a base da comunicação que existe em toda a Internet para serem encontrados mais facilmente pelo público através de um clique. Independentemente do servidor que escolha para hospedar, por exemplo, o site de sua empresa, haverá um programa projetado para receber solicitações *Hypertext Transfer Protocol* (HTTP). O navegador que utiliza para acessar esse site é um “cliente” que envia solicitações ao seu site hospedado pela sua escolha de servidor [Gourley e Totty 2002].

2.2.3 HTTPS: *Hypertext Transfer Protocol Secure* (HTTPS) é um protocolo de transferência segura, como o nome já diz, sua principal função é garantir que a URL acessada tenha de fato uma conexão segura entre servidores que hospedam um site e o seu dispositivo. Seu funcionamento é através da criptografia de dados. Para que a troca de informações seja segura, os dois servidores devem ser autenticados [Gourley e Totty 2002].

2.2.4 Proxy Reverso: Em rede de computadores, um proxy reverso básico fica entre um grupo de servidores e os clientes. Cliente é qualquer hardware ou software que pode enviar solicitações para um servidor, por exemplo, um navegador web.

Um proxy reverso fornece: segurança, balanceamento de carga e facilidade de manutenção. É simples de implementar e proporciona ao usuário segurança de ponta a ponta contra-ataques a servidores web como DDoS e DoS [Fraga 2019].

2.3 Mecanismos de ataque

Nesta sessão serão mostrados os dois tipos de mecanismos de ataque utilizados neste trabalho.

2.3.1 DoS: É um ataque de negação de serviço, com o objetivo de fazer com que aconteça uma sobrecarga em um servidor ou computador comum para que os recursos do sistema fiquem indisponíveis para quem os utiliza. Para isso, o invasor utiliza meios de enviar diversos pedidos (requisições) de pacotes para o alvo, com a finalidade de que este fique totalmente sobrecarregado e pare de responder, causando assim a negação dos serviços prestados [Fraga 2019].

2.3.2 DDoS: DDoS, o ataque ocorre de forma semelhante ao DoS, no entanto com algumas camadas extras. Um computador central chamado de 'mestre" gerencia uma série de outros computadores, conhecidos como "escravos" ou zumbis, assim esses escravos comandados pelo mestre (invadido por um hacker) atacam simultaneamente a vítima (servidor) sobrecarregando-o facilmente, causando a interrupção dos serviços [Fraga 2019].

2.3.3 LOIC: A ferramenta *Low Orbit Ion Cannon* (LOIC) é um software de computador de código aberto escrito em C#, com o objetivo de executar o ataque de negação de serviço. Foi desenvolvido pela Praetox Technologies em 2006, com o objetivo de avaliar e realizar testes de redes, faturamento foi liberado para o domínio público [Under Linux 2011].

2.4 Modelo de Referência OSI

O *Open Systems Interconnection (OSI)* é um modelo de referência e tem como objetivo ser um modelo padrão para protocolos de comunicações entre diversos tipos de sistemas garantindo a comunicação ponto a ponto, foi lançado em 1984 pela *International Organization for Standardization* (IOS).

Essa arquitetura divide as redes de computadores em 7 camadas: sessão física, dados, rede, transporte, sessão, apresentação e aplicação. Para obter camadas de abstração, cada protocolo realiza a inserção de uma funcionalidade assinalada a uma camada específica [Kurose e Ross 2002]. Apesar de existir 7 camadas no modelo OSI este trabalho tratará apenas de 3 camadas, que são as camadas que de fato são implementados mecanismos eficazes contra-ataques de negação de serviço em todo o mundo.

2.4.1 Camada de Rede

Camada responsável pelo endereçamento IP de origem e de destino, ela atua como uma controladora de roteamento entre a origem e o destino do pacote, assim como os correios, verificam a carta e o destinatário e quem é o remetente da mensagem. O endereço MAC é o endereço físico de quem envia o pacote, já o endereço IP é a identificação da sua máquina na rede [Kurose e Ross 2002].

2.4.2 Camada de Transporte: Camada responsável pelo envio e o recebimento dos pacotes vindos da camada 3, é nela que o gerenciamento do transporte é feito para garantir o sucesso do envio e no recebimento dos dados como se fossem os caminhões e os carteiros.

Os protocolos mais comuns nessa camada são os TCP e UDP. O protocolo TCP garante a entrega da mensagem e o UDP é muito mais rápido na entrega da mensagem, porém não garante a entrega [Kurose e Ross 2002].

2.4.3 Camada de Aplicação: Última camada do modelo OSI, é nela que os dados são consumidos, onde temos os programas que interagem com o humano, nela são exibidos e-mails, arquivos, websites etc. Nessa camada ficam os protocolos mais conhecidos como o HTTP, HTTPS, *File Transfer Protocol* (FTP), além de serviços como *Domain Name System* (DNS) [Kurose e Ross 2002].

3.Trabalhos Relacionados

Nesta sessão serão apresentadas propostas acadêmicas e soluções comerciais, abordando a proteção contra-ataques DoS e DDoS, explicando seu funcionamento e formas de se prevenir contra eles. Nas soluções comerciais é possível observar projetos concretizados e muito utilizados em todo o mundo, empresas gigantes como o Google, Amazon, Microsoft, cada uma delas possui um mecanismo de proteção contra-ataques que são comercializados ao mundo.

3.1 Propostas acadêmicas

3.1.1 A Practical Approach and Mitigation Techniques on Application Layer DDoS Attack in Web Server

Esse trabalho apresenta técnicas para a realização de ataques DoS e DDoS, seus impactos em um determinado site ou servidor, existem muitos jeitos de filtrar esses ataques no nível de rede, mas em um nível de aplicativo são mais difíceis de serem detectados. Cita o uso de uma ferramenta chamada Wireshark como um analisador de protocolos de rede, que é usado para capturar os pacotes durante um ataque DoS. Propõe o uso de um proxy web de código aberto chamado Nginx para a mitigação de ataques DoS e largura de banda [Arafat Yeasir 2015].

Após o Nginx ser implementado e devidamente configurado, são realizadas simulações para medir o desempenho da ferramenta na mitigação dos ataques DDoS na camada de aplicativo no servidor Web, esses testes são vistos através da entrada de tráfego HTTP no Wireshark.

3.1.2 Distributed Defense Against DDoS Attacks

Este projeto investiga uma solução cooperativa para o problema de ataques distribuídos de negação de serviço. O sistema de defesa proposto, DefCOM, combina as vantagens das defesas da extremidade da vítima (detecção precisa de ataques) e das defesas da extremidade da origem (resposta eficiente e separação precisa do tráfego legítimo do tráfego de ataque). Ele também conta com a ajuda de roteadores de backbone para controlar o tráfego de ataque em cenários de implantação parcial, onde muitas fontes potenciais não implantam uma defesa de origem-fim [Mirkovic 2005].

DefCOM constrói uma rede par a par distribuída de nós de defesa cooperativa espalhados pela Internet. Nós de defesa trocam informações e controle de mensagens para detectar ataques e responder coletivamente garantindo um bom serviço para o tráfego legítimo. Eles diferenciam entre legítimo e ataque pacotes, dedicar sua largura de banda disponível para o tráfego legítimo e cooperar com outros nós de defesa para garantir um bom serviço aos clientes legítimos.

3.1.3 Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions

O seguinte trabalho explica o que é um ataque DoS e DdoS, métodos e mecanismos para o lançamento de um ataque, métodos de prevenção, métodos de detecção [Bhatia 2018].

Um DoS, ataque de negação de serviço, é uma tentativa deliberada e maliciosa de um adversário de interromper intencionalmente as operações normais de um provedor de serviços, ou um servidor, tornando seus recursos indisponíveis para os clientes pretendidos.

Ataques maiores chamados DDoS, ataque de negação de serviço distribuído, utiliza uma série de máquinas dispersas que estão comprometidas (também conhecidas como zumbis, bots ou escravos) que são controladas por um atacante (bot-master), é utilizado contra um alvo específico para causar uma negação de serviços. A rede de máquinas comprometidas é denominada de botnet. A diferença do DDoS é que ele utiliza da capacidade individual de cada máquina comprometida para ampliar os efeitos contra uma vítima em comum, ampliando assim, o efeito.

3.2 Soluções Comerciais

3.2.1 Cloudflare

A solução de proteção contra DDoS da Cloudflare protege sites, aplicações e redes inteiras, garantindo que o desempenho do tráfego legítimo não seja comprometido. A Rede de 90 Tbps da Cloudflare bloqueia uma média de 87 bilhões de ameaças por dia, incluindo alguns dos maiores ataques de DDoS da história.

Segundo a Forrester, no primeiro trimestre de 2021, a Cloudflare foi nomeada “Lider de Mercado”, ela protege contra-ataques Ddos a partir da borda e com rapidez. A mitigação de DDoS nos servidores de todas as cidades e todos os data centers da Cloudflare que abrangem 200 cidades em 100 países, executam a pilha completa de serviços de mitigação de DDoS. Os sistemas de mitigação centralizados e descentralizados trabalham em conjunto para identificar e mitigar a maioria dos ataques DDoS em menos de 3 segundos e regras estáticas pré-configuradas são implementadas em menos de 1 segundo [Cloudflare 2021].

3.2.2 Microsoft Azure

A Microsoft investe mais de 1 bilhão de dólares anualmente em pesquisa e desenvolvimento de segurança cibernética. Empregam mais de 3500 especialistas em segurança dedicados à privacidade e à segurança dos dados.

Possui proteção de multicamada, implantada com o firewall do aplicativo web do gateway de aplicativo do Azure, esta proteção contra DDoS é feita através da camada 3 e 4 e utiliza a camada 7 (camada de aplicativo) como injeção SQL através de scripts intersite. Esse Firewall do aplicativo web é pré-configurado para lidar com as 10 vulnerabilidades mais comuns. Conta com um sistema de análise do ataque, onde poderá obter relatórios detalhados durante um ataque e transmitir logs de fluxo de mitigação de DDoS para um sistema de SIEM (gerenciamento de eventos e informações de segurança) para monitorar o ataque quase que em tempo real [Microsoft 2021].

3.2.3 AMAZON (AWS SHIELD)

É um serviço gerenciado de proteção contra DDoS que protege os aplicativos executados na AWS. O AWS Shield oferece detecção e mitigações em linha automáticas e sempre ativas que minimizam o tempo de inatividade e a latência dos aplicativos e possui dois níveis o Standard e Advanced. A versão Standard protege contra os ataques de DDoS mais comuns.

Esses ocorrem com frequência nas camadas de rede e transporte e visam sites ou aplicativos web. Ao utilizar o AWS Shield Standard com o Amazon CloudFront e o Amazon Route 53, receberá uma proteção mais abrangente de disponibilidade contra todos os ataques conhecidos de infraestrutura (camada de rede (3) e de transporte (4)). Já a versão Advanced oferece detecção e mitigação adicionais contra-ataques grandes e sofisticados de DDoS, visibilidade praticamente em tempo real aos ataques e integração ao AWS WAF, um firewall para aplicação WeB, além de acesso 24 horas, 7 dias na semana ao AWS Shield Response Team (STR) [Amazon 2021].

3.2.4 Google Cloud Armor

O Cloud Armor aproveita a experiência de proteção das principais propriedades da Web, com a pesquisa Google, Gmail e YouTube, além disso, promove defesas integradas contra DDoS nas camadas Física e Transporte. Possui a vantagem de reduzir os 10 principais riscos do *Open Web Application Security Project* (OWASP).

Possui normas predefinidas para ajudar na proteção contra-ataques cibernéticos, como scripting em vários locais (XSS) e injeção de SQL (SQLi). Utilizando as políticas de segurança do Cloud Armor, permitir ou negar acesso ao balanceador de carga HTTP(s) externo na borda do Google Cloud, o mais próximo possível da origem do tráfego de entrada [Google 2021].

3.3 Análise dos trabalhos relacionados

Analisando os trabalhos relacionados é possível observar um objetivo em comum, ou seja, a tentativa de bloquear ataques de negação de serviço utilizando diferentes métodos, desde a proteção física até níveis de aplicação.

A principal característica desses trabalhos é demonstrar diferentes técnicas de proteção e mitigação contra-ataques DoS e DDoS. No primeiro trabalho citado é possível observar dois métodos de proteção, o próprio Nginx e o Apache, já o segundo é proposto um método de proteção corporativo distribuído chamado DefCOM que aborda a proteção de borda, do alvo e do invasor. O último trabalho aborda o funcionamento de um ataque DDoS, e como diversas máquinas afetadas trabalham em conjunto para atacar seu verdadeiro alvo.

4.Proposta

O Brasil está entre os países mais vulneráveis do mundo em relação a cibersegurança. De acordo com Bellio (2021) mais da metade das empresas brasileiras estão vulneráveis a ataques virtuais, com um custo de 1,35 milhões de dólares de prejuízo em média as empresas sofrem com invasões de dados [Empresas & Negócios 2021].

Diante dessa necessidade de mercado e com base nos trabalhos citados no referencial teórico, este projeto propõe a implementação de um web-proxy conhecido como Nginx para atuar como proxy-reverso e controlador de tráfego, a fim de bloquear, mitigar e monitorar possíveis ataques a um determinado servidor. Nesse caso, uma empresa que utilizasse a solução proposta neste trabalho poderia minimizar os riscos de ter os seus serviços online interrompidos.

A Figura 1, no segundo cenário representa a proposta deste trabalho, onde há um invasor/hacker que irá disparar um ataque planejado em dois servidores diferentes, o primeiro é apenas um servidor comum e não dispõe de proteções avançadas, já o segundo conta com a proteção de um proxy-reverso conhecido como Nginx para o

redimensionamento e balanceamento de carga. Esse bloqueio é feito através de configurações em um servidor que está instalado, o nginx, e este controla o tráfego na rede, o que pode ou não deve passar, controlando IP's seguros conhecidos como "TrustedHosts" para passarem sem intervenção.

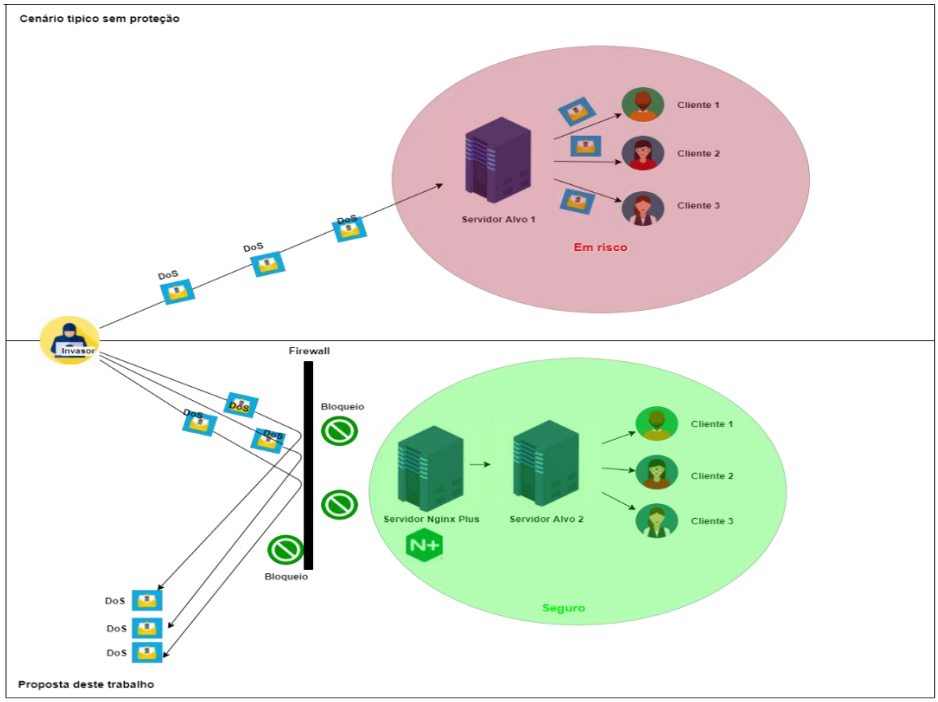


Figura 1. Proposta de projeto (Autor)

Conforme pode ser observado na Figura 1 há a representação de dois cenários. Na primeira parte é um modelo típico totalmente sem proteção. Já, na segunda parte, há a inserção de técnicas de mitigação.

Considerando esses dois cenários, no primeiro há algumas vantagens como velocidade do serviço, porém há riscos de segurança. Já na proposta apresentada por este trabalho há a inserção de algumas técnicas de mitigação que visam, justamente, corrigir/solucionar essas brechas do primeiro cenário, logo, a segurança é ampliada, mas outras partes são afetadas como a velocidade dos serviços prestados. Porém essa arquitetura composta por essas técnicas, quando há uma invasão, essa ferramenta Nginx atua como um firewall, barrando conexões suspeitas e limitando a passagem de dados ao servidor principal, dessa maneira, apenas conexões seguras são permitidas a passar pela barreira, o que causa maior lentidão, porém melhor segurança.

5. Padrões de execução de testes de penetração

Diante da necessidade de mercado e considerando também os trabalhos relacionados, este trabalho irá utilizar a metodologia *The Penetration Testing Execution Standard* (PTS), que é um padrão de execução de teste de penetração que consiste em 7 etapas principais. Essas etapas englobam os processos relacionados a um teste de penetração, desde comunicação inicial e todo o raciocínio por trás de um *pentest* [PTES 2021]. Essas etapas são classificadas como:

(i) primeira etapa: consiste na interação de pré-engajamento e o objetivo é apresentar e explicar as ferramentas e técnicas disponíveis para auxiliar na primeira etapa de um teste de penetração. O escopo deve ser definido, a forma como cada aspecto do teste será conduzida;

(ii) segunda etapa: consiste na coleta de informações, onde serão definidas as atividades da coleta de inteligência de um teste de penetração. Seu objetivo é propor um padrão projetado especificamente para o testador (aquele que realiza o ataque) realizar o reconhecimento contra um alvo (corporativo, militar, ou algo relacionado), nessa etapa é detalhado o processo de pensamento e os objetivos do reconhecimento de um teste de penetração.

(iii) terceira etapa: consiste na modelagem de ameaças, conforme necessário para a execução do teste, esse padrão não utiliza um modelo específico, mas exige que o modelo seja consistente no que diz respeito a sua representação de ameaças, suas capacidades e qualificações de acordo com a organização que será testada.

(iv) quarta etapa: trata da análise de vulnerabilidade, o processo de descoberta de falhas de um sistema e aplicativos que possam ser aproveitados por um invasor, essas falhas englobam desde a configuração incorreta de hosts ou serviços até design de aplicativos inseguros.

(v) quinta etapa: denominada exploração e consiste exclusivamente em estabelecer o acesso a um sistema ou recurso, contornando as restrições de segurança, seu principal foco é identificar o ponto de entrada na organização e identificar alvos de alto valor.

(vi) sexta etapa: chamada pós-exploração e é nela onde é determinado o valor da máquina comprometida e manter o controle dela para o uso posterior. Esse valor é determinado pela sensibilidade dos dados armazenados nela e pela utilidade da máquina em comprometer ainda mais a rede.

(vii) sétima etapa: consiste em relatar os critérios básicos para o teste de penetração, como um resumo executivo, a postura geral, sua classificação, perfil de risco e as descobertas gerais, bem como um relatório técnico dos testes.

Considerando o cenário de aplicação da presente proposta, este trabalho utilizará as etapas de exploração, pós-exploração e relatórios. As demais etapas não serão exploradas neste trabalho, pois não serão objetos de estudo.

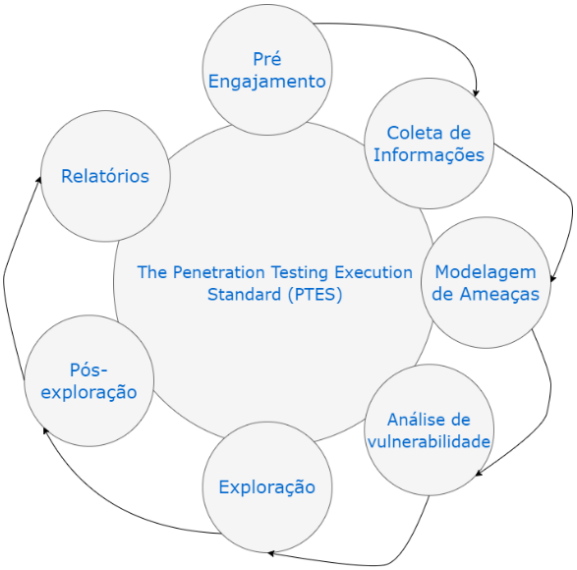


Figura 2. Metodologia PTES (PTES 2021)

6. Metodologia

Na sessão 6.1 foi tratado a metodologia implementada neste trabalho.

6.1 Cenário de validação e testes

O cenário de validação e testes será configurado utilizando quatro máquinas físicas (S) e uma máquina virtual (M). Primeiramente uma das máquinas físicas será utilizada para os testes de invasão e estará em uma rede separada da máquina virtual, já a máquina virtual, será utilizada para a hospedagem dos servidores alvos e para o Nginx. Primeiramente será a M1 e estará totalmente exposta a Internet, após realizados testes na máquina M1, a mesma será utilizada e instalado o servidor de proxy-reverso Nginx Plus que atuará como balanceador de carga.

A máquina virtual (M1) terá um serviço de consulta a uma base de dados MySql, que será disponibilizada aos clientes através de uma página web exibida pelo PHP. Os testes serão realizados medindo o tempo de resposta da página web durante a realização dos ataques, utilizando recursos como o Ping.

Utilizando uma máquina física S2, será disparado um ataque DoS, utilizando o protocolo TCP ou UDP, em direção ao IP do M1, através da ferramenta de ataque LOIC. O M1 será monitorado por meio da ferramenta de monitoramento Wireshark para o reconhecimento e confirmação do ataque, após a realização dos testes e a coleta de informações o cenário da máquina virtual M1, será moldado para a proposta deste trabalho.

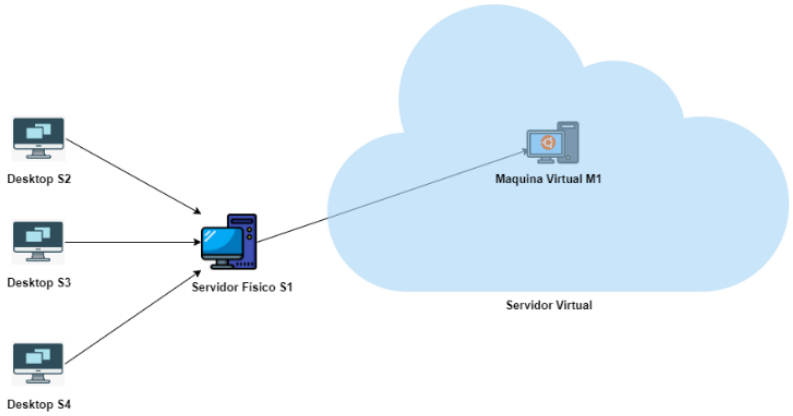


Figura 3. Cenário de Testes Típico (Autor)

Outro ataque DoS utilizando a ferramenta LOIC foi disparado em direção a máquina virtual M1, onde estará agora localizado o Nginx Plus, que também será monitorado pelo Wireshark.

Através do primeiro teste o ataque DoS tornou os serviços da M1 instáveis e derrubou a conexão com qualquer cliente que esteja acessando seus serviços. Já no segundo teste, é previsto que o Nginx identifique o excesso de carga sendo disparado e bloqueie o ataque, deixando assim os serviços prestados pela M1 a qualquer cliente intacto.

Um novo ataque DDoS foi lançado aos servidores alvos utilizando também a ferramenta LOIC, três máquinas físicas S2, S3 e S4 serão usados simulando assim múltiplos computadores atacando um mesmo servidor, no primeiro caso, é esperado que derrube seus serviços, visto que um simples ataque já havia feito, já no segundo caso é

esperado que o Nginx Plus não consiga bloquear totalmente o ataque devido a magnitude dele, mas apenas uma parte.

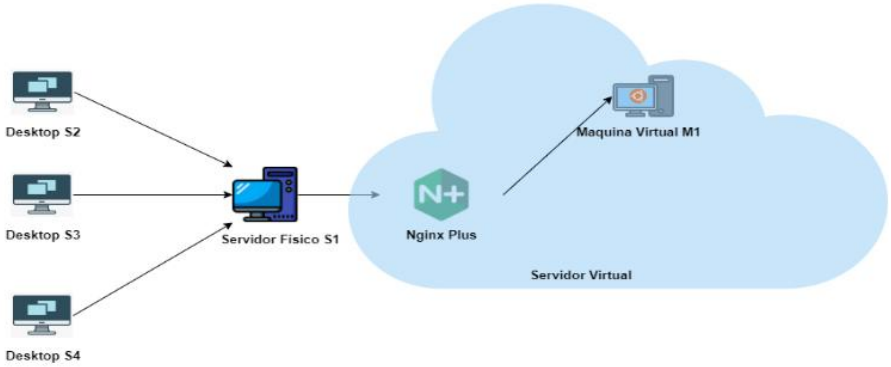


Figura 4. Cenário de Testes Nginx Plus (Autor)

6.1 Cenário de testes sem proteção

6.1.1 Considerações iniciais

O link de Internet onde foi hospedado o servidor de acesso aos clientes possui 300Mb/s de Download e 150 Mb/s de Upload, já o link utilizado para a realização dos ataques possui 100Mb/s de Download e Upload.

Utilizando a ferramenta LOIC foi disparado um ataque DoS, em direção ao endereço onde a consulta é disponibilizada aos clientes (http://bruno.avmb.com.br/consulta.php), usando o protocolo TCP, conforme a imagem abaixo.

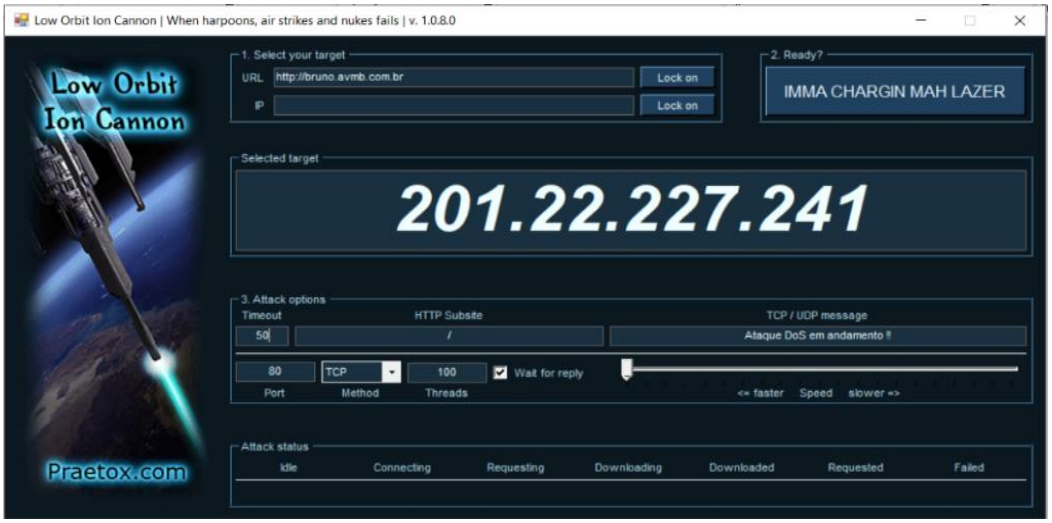
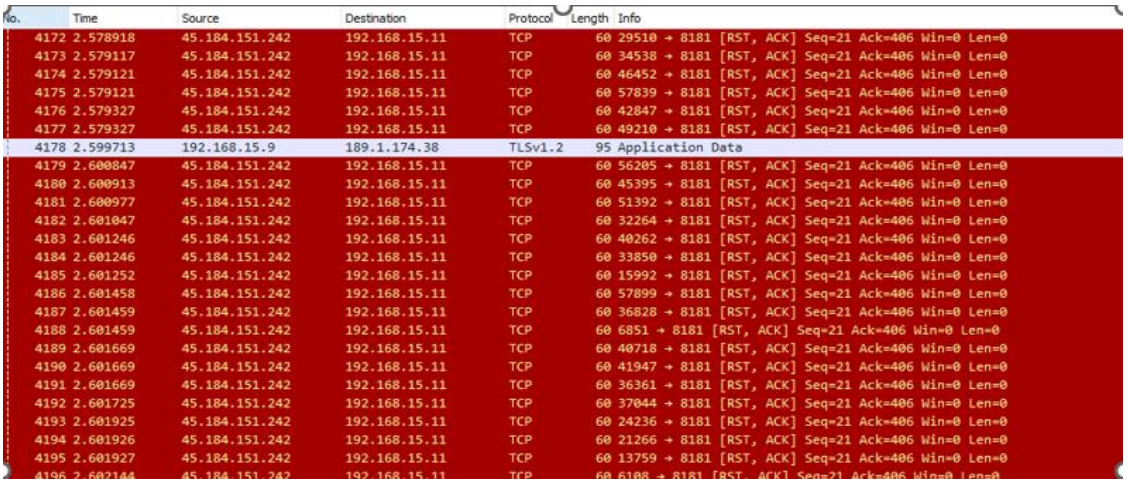


Figura 5. Loic TCP 80 (Autor)



No.	Time	Source	Destination	Protocol	Length	Info
4172	2.578918	45.184.151.242	192.168.15.11	TCP	60	29510 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4173	2.579117	45.184.151.242	192.168.15.11	TCP	60	34538 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4174	2.579121	45.184.151.242	192.168.15.11	TCP	60	46452 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4175	2.579121	45.184.151.242	192.168.15.11	TCP	60	57839 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4176	2.579327	45.184.151.242	192.168.15.11	TCP	60	42847 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4177	2.579327	45.184.151.242	192.168.15.11	TCP	60	49210 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4178	2.599713	192.168.15.9	189.1.174.38	TLSv1.2	95	Application Data
4179	2.600847	45.184.151.242	192.168.15.11	TCP	60	56205 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4180	2.600913	45.184.151.242	192.168.15.11	TCP	60	45395 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4181	2.600977	45.184.151.242	192.168.15.11	TCP	60	51392 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4182	2.601047	45.184.151.242	192.168.15.11	TCP	60	32264 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4183	2.601246	45.184.151.242	192.168.15.11	TCP	60	40262 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4184	2.601246	45.184.151.242	192.168.15.11	TCP	60	33850 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4185	2.601252	45.184.151.242	192.168.15.11	TCP	60	15992 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4186	2.601458	45.184.151.242	192.168.15.11	TCP	60	57899 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4187	2.601459	45.184.151.242	192.168.15.11	TCP	60	36828 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4188	2.601459	45.184.151.242	192.168.15.11	TCP	60	6851 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4189	2.601669	45.184.151.242	192.168.15.11	TCP	60	40718 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4190	2.601669	45.184.151.242	192.168.15.11	TCP	60	41947 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4191	2.601669	45.184.151.242	192.168.15.11	TCP	60	36361 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4192	2.601725	45.184.151.242	192.168.15.11	TCP	60	37044 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4193	2.601925	45.184.151.242	192.168.15.11	TCP	60	24236 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4194	2.601926	45.184.151.242	192.168.15.11	TCP	60	21266 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4195	2.601927	45.184.151.242	192.168.15.11	TCP	60	13759 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0
4196	2.602144	45.184.151.242	192.168.15.11	TCP	60	6108 → 8181 [RST, ACK] Seq=21 Ack=406 Win=0 Len=0

Figura 6. Solicitações Wireshark (Autor)

A Figura 6 representa algumas solicitações vindas do IP do atacante em direção ao IP do servidor alvo, utilizando o protocolo TCP, como é possível observar esses ataques chegam ao servidor onde está hospedado o serviço fornecido aos clientes.

A Figura 7 representa um Ping utilizando um buffer de 65500 bytes (tamanho máximo permitido pelo Prompt de Comando), em direção ao site (http://bruno.avmb.com.br/consulta.php) no momento do Ping não havia nenhum ataque em andamento.

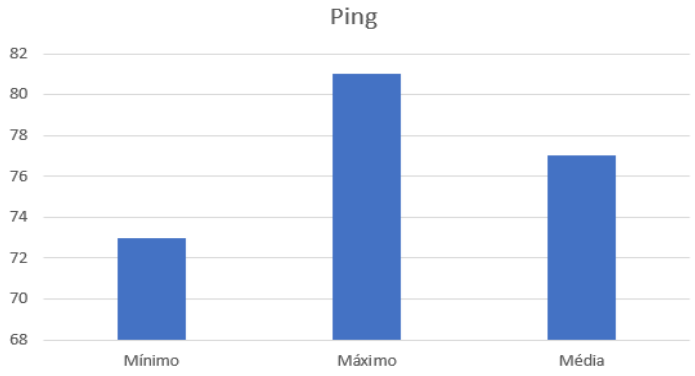


Figura 7. Ping sem ataques (Autor)

A Figura 8 representa uma solicitação de Ping também com 65500 bytes de buffer, 1 ataque DoS em andamento, os números a esquerda estão em milissegundos (ms), uma máquina física S2, utilizando o protocolo TCP para o ataque ao site (http://bruno.avmb.com.br/consulta.php).

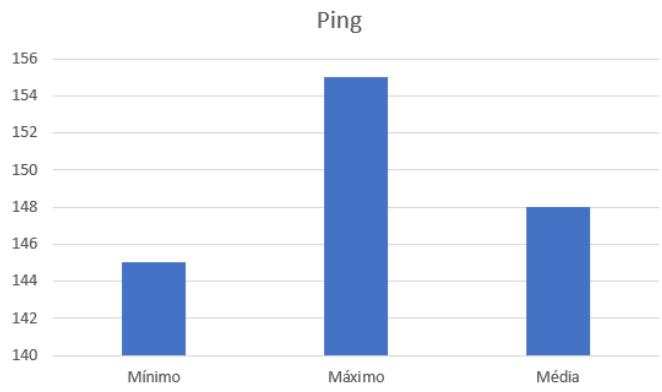


Figura 8. Ping com 1 ataque (Autor)

A Figura 9 representa 2 ataques simultâneos utilizando dois computadores físicos S2, S3, em direção ao site citado acima, os números a esquerda estão em milissegundos (ms). O ataque possui as mesmas características das especificações descritas na Figura 8, porém duplicado.

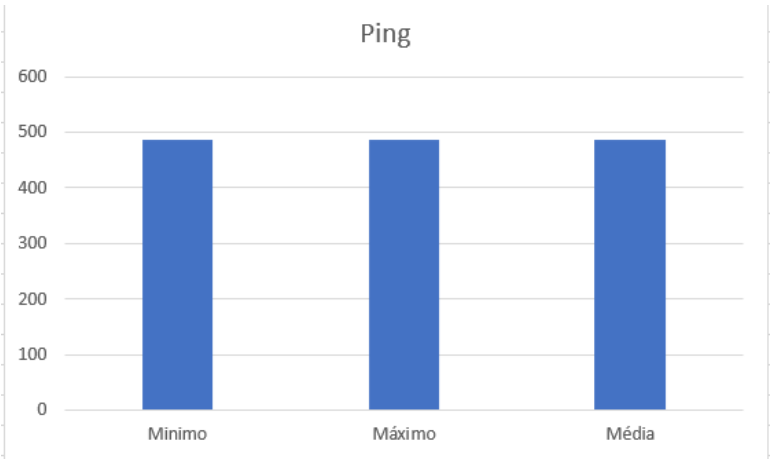


Figura 9. Ping com 2 ataques (Autor)

Utilizando três computadores físicos, S2, S3 e S4, foi possível causar Timeout em todas as solicitações e causando em um total de 4 Pings a perda de 4 pacotes, demostrado abaixo pela Figura 10.

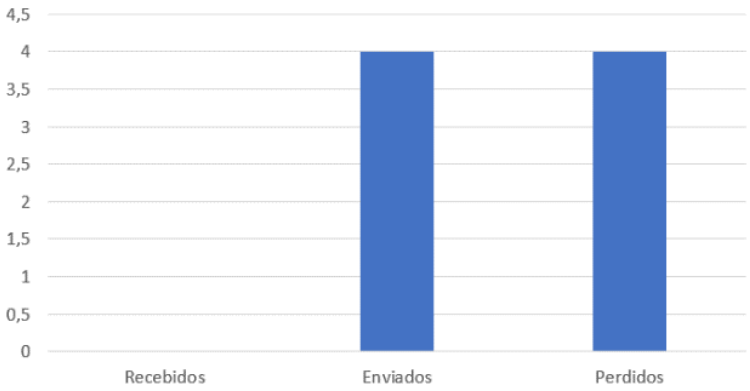


Figura 10. Pacotes com 3 ataques (Autor)

O protocolo TCP que foi utilizado para o ataque DoS e DDoS, foi utilizado para os testes demonstrados das Figuras 7 à 10, é possível observar que com apenas 3 ataques simultâneos foi possível causar Timeout total no site onde os clientes utilizam para fazer consultas ao banco de dados, isto porque o protocolo TCP é voltado à conexão e garante a integridade e ordem de todos os dados utilizando *Three way handshake* (aperto de mãos de três vias), também conhecido como SYN, SYN-ACK,ACK.

Enquanto utilizando o protocolo UDP apenas uma máquina física (S2) foi capaz de realizar completamente Timeout ao servidor, enquanto o ataque não cessar o servidor não foi capaz de responder as solicitações de Ping, isto porque no protocolo UDP não é necessário estabelecer uma comunicação tornando-o assim muito veloz e permite uma comunicação bastante rápida, mesmo perdendo alguns dados na comunicação.

6.2 Cenário de testes com Nginx Plus

Com a instalação do Nginx Plus e efetivação da configuração e as devidas proteções como HTTPS, Load Balance e limite de conexões simultâneas ao serviço de consulta disponibilizado pelo PHP aos clientes.

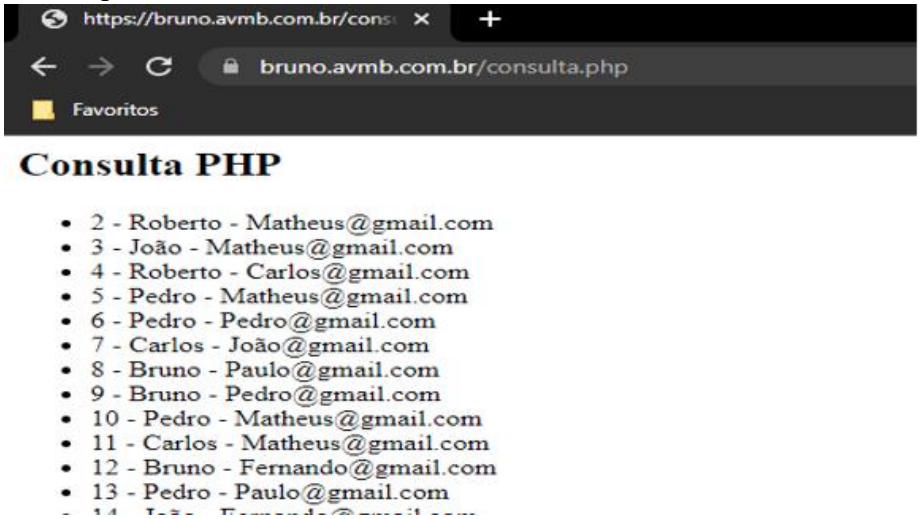


Figura 11. Consulta via HTTPS (Autor)

A Figura 11 representa a consulta disponibilizada aos clientes, utilizando HTTPS, deixando a conexão mais segura. Os dados foram gerados de forma aleatória, pois a consulta possui 11 mil linhas.

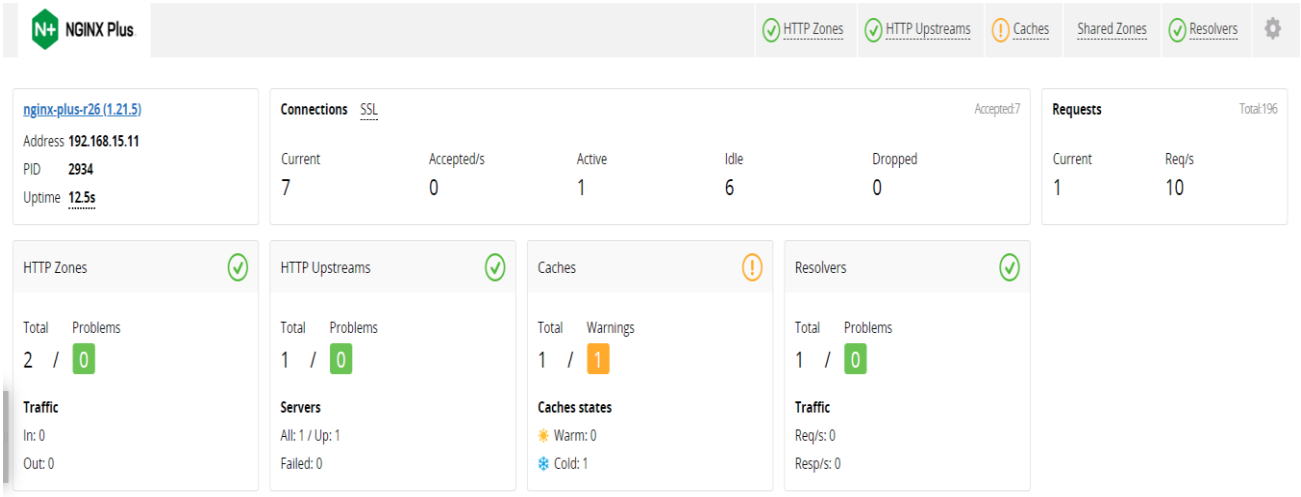


Figura 12. Dashboard Nginx Plus (Autor)

A Figura 12 mostra o dashboard do Nginx Plus, configurado com zonas de *Upstream* que limitam a passagem de largura de banda a serviços disponibilizados em portas.

Figura 13. Conexões instantâneas (Autor)

A Figura 13 mostra o status das conexões instantâneas ao servidor, sem ataques, apenas acessos.

Mudando para a porta padrão do SSL (HTTPS) 443 onde a consulta está sendo disponibilizada, e lançando mais uma vez outro ataque DoS, é possível visualizar na imagem abaixo as solicitações chegando no Nginx.

Figura 14. Conexões durante o ataque (Autor)

As solicitações podem chegar de qualquer lugar, nenhum IP específico foi bloqueado, por isso não aparecerá em recusados (Dropped) apenas serão limitadas as requisições conforme a Figura 14 mostra.

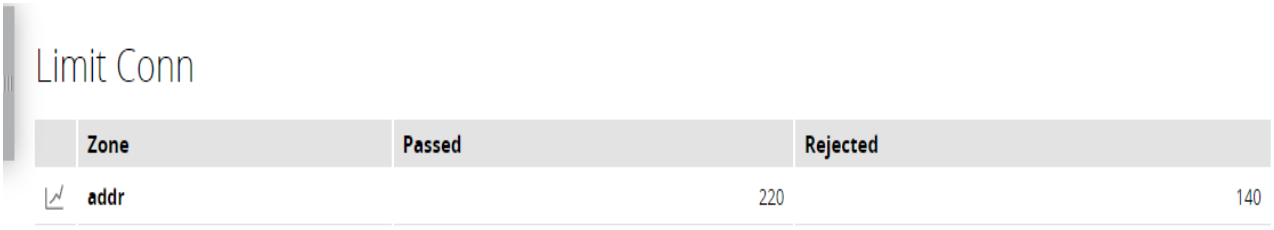


Figura 15. Conexões Limitadas (Autor)

No momento do ataque devido a configuração do Nginx, em uma total de 360 conexões, 220 passaram e 140 foram rejeitadas pelo limitador.

Durante os ataques DoS e DDoS com as máquinas físicas S2, S3 e S4, utilizadas anteriormente para atacar o cenário sem proteção, enquanto utilizar os protocolos TCP e HTTP, tanto DoS (S2) ou DDoS (S2, S3 e S4) o serviço entregue pela URL (https:/bruno.avmb.com.br/consulta.php) aos clientes não oscilou em nenhum momento durante os ataques.

Quando mudamos o ataque para utilizar o protocolo UDP a conexão fornecida pela URL cai instantaneamente, pois não foi configurado no Nginx Plus, um balanceamento para o protocolo UDP, e como no modem não foi configurado rotas para o protocolo UDP, o mesmo é inundado de solicitações causando o travamento do link de Internet e a negação de serviço.

8. Conclusões Finais

Ataques DoS e DDoS são uma ameaça significativa na Internet, são comumente realizados através de simples ferramentas disponíveis na internet de forma gratuita. A partir desses ataques é possível causar desde indisponibilidade em um sistema até mesmo possível exploração de dados de uma organização e como os ataques são difíceis de serem detectados ou analisados é um fator importante para que continuem acontecendo com mais frequência.

Neste trabalho foi realizado a comparação de diferentes cenários de testes, utilizando ataques DoS e DDoS em ambos os cenários, no primeiro cenário os ataques DoS e DDoS atingiram o alvo e causaram lentidão e a negação de serviço. Já no segundo cenário os ataques DoS e DDoS não conseguiram atingir o alvo utilizando o protocolo TCP e HTTP, porém causou a negação de serviço utilizando o UDP, pois não foi implementado nas zonas de defesas do Nginx Plus proteção contra UDP.

Através da ferramenta Wireshark foi possível identificar os ataques acontecendo em tempo real e identificar o IP do invasor e colocá-lo na blacklist do Nginx, para que futuramente ataques da mesma fonte não venham a se repetir.

9.Referências

Amazon, Web Services, Inc (2021) “AWS Shield”, https://aws.amazon.com/pt/shield/, Setembro.

Arafat Yeasir, Muhammad. (2015) “A Practical Approach and Mitigation Techniques on Application Layer DDoS Attack in Web Server”, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.734.8119&rep=rep1&type=pdf, Setembro.

Bullock, Jessey e Parker, Jeff. (2017) “Wireshark para Profissionais de Segurança”, 1ª Edição, Editora Novatec.

Boavida, Fernando. (2012) “TCP/IP. Teoria e Prática”, Editora Fca, 1ª Edição.

Bhatia, Sajal. (2018) “Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions”, https://www.researchgate.net/publication/328347710_Distributed_Denial_of_Service_Attacks_and_Defense_Mechanisms_Current_Landscape_and_Future_Directions, Setembro.

Chappell, Laura. (2010) “Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide”, Second Edition.

Cloudflare, Inc (2021) “Proteção contra-ataques enterprise DDoS”, https://www.cloudflare.com/pt-br/, Setembro.

DeJonghe, Derek. (2021) “NGINX Cookbook: Advanced Recipes for High-Performance Load Balancing”, Updated Edition.

Devmedia, Christiane. (2015) “Wireshark: Analisando o tráfego de redes”, https://www.devmedia.com.br/wireshark-analisando-o-trafego-de-redes/29616, Setembro.

Fraga, Bruno. (2019) “Técnicas de Invasão: Aprenda as Técnicas usadas por hackers em invasões reais”, Compilado por Thompson Vangller.

Gourley, David e Totty, Brian. (2002) “HTTP: The definitive Guide”, Edited for O’ Reilly 2002.

Google, Cloud (2021) “Google Cloud Armor”, https://cloud.google.com/armor, Setembro.

Kurose, James e Ross, Keith. (2002) “Redes de Computadores e a Internet: Uma nova abordagem”, 1ª Edição.

Linux, Under (2011) “LOIC: Ferramenta para Ataques DoS/DDoS”, https://under-linux.org/content.php?r=2809, Outubro.

Microsoft, (2021) “Azure DDoS Protection”, https://azure.microsoft.com/pt-pt/services/ddos-protection/, Setembro.

Mirkovic, Jelena. (2005) “Distributed Defense Against DDoS Attacks”, https://www.isi.edu/~mirkovic/publications/udel_tech_report_2005-02.pdf, Setembro.

PTES, Team (2021) “The Penetration Testing Execution Standard Documentation”, https://buildmedia.readthedocs.org/media/pdf/pentest-standard/latest/pentest-standard.pdf, Outubro.