INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS PEDRO II - PI
TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

FRANCISCO EDUARDO DE SOUSA MONTEIRO

COMPARAÇÃO E ANÁLISE DE DESEMPENHO DAS FERRAMENTAS DE ATAQUE DDoS: SLOWLORIS, GOLDENEYE, XERXES E TORSHAMMER

PEDRO II

2024

FRANCISCO EDUARDO DE SOUSA MONTEIRO

COMPARAÇÃO E ANÁLISE DE DESEMPENHO DAS FERRAMENTAS DE ATAQUE DDoS: SLOWLORIS, GOLDENEYE, XERXES E TORSHAMMER

Trabalho de Conclusão de Curso (artigo científico) apresentado como exigência parcial para obtenção do diploma do Curso de Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Pedro II.

Orientador: Prof. Esp. Cléber da Silva Araújo.

PEDRO II

2024

COMPARAÇÃO E ANÁLISE DE DESEMPENHO DAS FERRAMENTAS DE ATAQUE DDoS: SLOWLORIS, GOLDENEYE, XERXES E TORSHAMMER

Francisco Eduardo de Sousa Monteiro[1]
Cléber da Silva Araújo[2]

RESUMO

Com o avanço constante do uso da Internet em diversos setores, como comércio, educação, governo e uso pessoal, a segurança da informação tem se tornado uma questão relevante e desafiadora. Neste contexto, os ataques de negação de serviço (DoS) e os ataques de negação de serviço distribuídos (DDoS) têm se destacado como uma das principais ameaças enfrentadas atualmente. Diante disso, é essencial avaliar e comparar a força do ataque DoS/DDoS lançado por estas ferramentas para conceber contramedidas eficientes contra eles. Neste artigo, o desempenho de quatro ferramentas de ataque DoS/DDoS é comparado e analisado usando parâmetros como tempo para lançar o ataque com sucesso, taxa de tráfego e tamanho do pacote. As ferramentas DoS/DDoS consideradas para avaliação são Slowloris, GoldenEye, Xerxes e Torshammer. Os resultados experimentais inferem que o Xerxes supera as outras ferramentas no lançamento de um ataque DoS/DDoS.

Palavras-chave: Negação de serviço; DDoS; Segurança.

ABSTRACT

With the constant advancement of Internet use in various sectors, such as commerce, education, government and personal use, information security has become a relevant and challenging issue. In this context, denial of service attacks (DoS) and distributed denial of service attacks (DDoS) have stood out as one of the main threats currently faced. Given this, it is essential to evaluate and compare the strength of the DoS/DDoS attack launched by these tools to design efficient countermeasures against them. In this article, the performance of four DoS/DDoS attack tools is compared and analyzed using parameters such as time to successfully launch the attack, traffic rate, and packet size. The DoS/DDoS tools considered for evaluation are Slowloris, GoldenEye, Xerxes and Torshammer. Experimental results infer that Xerxes outperforms other tools in launching a DoS/DDoS attack.

Keywords: Denial of service; DDoS; Security.

Data de aprovação: 10/01/2024 (data de apresentação do TCC)

1 INTRODUÇÃO

Com o avanço constante do uso da Internet em diversos setores, como comércio, educação, governo e uso pessoal, a segurança da informação tem se tornado uma questão relevante e desafiadora. Nesse contexto, um dos principais desafios é lidar com os ataques cibernéticos, que representam uma ameaça constante para indivíduos, organizações e até mesmo para a infraestrutura digital de um país (DUO; ZHOU; ABUSORRAH, 2022).

[1] Graduação em Análise e Desenvolvimento de Sistemas. IFPI. duuhmonteiro06@gmail.com
[2] Bacharelado em Ciência da Computação. UESPI. cleber.araujo@ifpi.edu.br

Dentre os diferentes tipos de ataques cibernéticos, os ataques de negação de serviço (DoS) e os ataques de negação de serviço distribuídos (DDoS) têm se destacado como uma das principais ameaças enfrentadas atualmente. Esses ataques são capazes de sobrecarregar os sistemas-alvo, tornando-os inoperantes e causando interrupções significativas nas atividades normais. Os danos resultantes de um ataque DoS/DDoS bem-sucedido podem ser devastadores, podendo levar a prejuízos financeiros, danos à reputação e até mesmo comprometimento da segurança dos dados (CARL et al., 2006).

De acordo com estatísticas recentes, um levantamento de dados realizado em 2020 revelou que o Brasil foi alvo de mais de 8,4 bilhões de tentativas de ataques cibernéticos. Esse número representa um pouco mais de 20% do total de casos registrados em toda a América Latina, somando cerca de 41 bilhões de casos (CLARINDO; SILVA, 2022).

No Brasil, a legislação referente a ataques DoS e DDoS leva em consideração as especificidades de cada ocorrência. Para ser considerado crime, um ataque DoS/DDoS deve causar danos significativos, como a interrupção do funcionamento normal de um sistema ou site específico (BRASIL, 2012; BRASIL, 1940; BRASIL, 2014).

Os dados estatísticos sobre os incidentes de ataques mencionados demonstram que o DoS/DDoS se tornou uma ameaça cibernética amplamente difundida (KUMAR; CARLEY, 2016). Assim, torna-se crucial aprofundar o estudo, a análise e o entendimento desse tipo de ataque por meio das ferramentas comumente utilizadas para essa finalidade.

Os ataques DoS/DDoS têm como objetivo sobrecarregar recursos como cache, memória principal, tempo de processamento da CPU e largura de banda de uma conexão de rede, tornando-os inacessíveis aos usuários finais e interrompendo a comunicação da rede, ou negando o acesso a esses serviços (YIN; ZHANG; YANG, 2018). Embora essas ferramentas tenham sido inicialmente desenvolvidas para testes de estresse em redes, atualmente, são utilizadas de maneira maliciosa por hackers para lançar ataques DDoS (CHOI et al., 2014). O objetivo geral dessa pesquisa é conduzir uma análise comparativa entre as ferramentas de ataque DoS/DDoS Slowloris, GoldenEye, Xerxes e Torshammer, com a avaliação de variáveis como o tempo necessário para a efetiva execução do ataque, a taxa de tráfego, o tamanho dos pacotes e os protocolos explorados, obtendo uma compreensão mais aprofundada do comportamento individual de cada uma dessas ferramentas.

Este trabalho apresenta as seguintes contribuições para o tema de pesquisa:

- Investigar os tipos de ataques DoS/DDoS mais comuns;
- Analisar o comportamento desses ataques;
- Avaliar o desempenho em termos de vários parâmetros de ataque;
- Obter insights para soluções de segurança nas corporações;

O presente trabalho está organizado da seguinte forma. A subseção 1.1 é apresentado um resumo dos mecanismos de defesa contra DoS/DDoS, conforme documentado na literatura. A seção 2 apresenta os conceitos fundamentais necessários para compreensão deste projeto. A Seção 3 apresenta a metodologia empregada para realização deste projeto de pesquisa. Apresenta-se na Seção 4 os Experimentos e resultados obtidos ao longo do projeto. E por fim a Seção 5, a conclusão para recapitular e destacar os principais pontos, descobertas e contribuições do estudo de pesquisa.

1.1 TRABALHOS RELACIONADOS

Na presente subseção, são abordados resumo dos mecanismos de defesa contra DoS/DDoS, conforme documentado na literatura, sendo que a Tabela 1 destaca os principais artigos relacionados, bem como suas ênfases e distinções em relação ao estudo proposto neste trabalho.

Tabela 1 - Trabalhos Relacionados

Publicação	Ano	Temática
Chahal *et al.* (CHAHAL; KAUR; SHARMA, 2021)	2021	Fornece uma visão abrangente dos desafios e soluções para a defesa contra ataques DDoS em ambientes SDN.
Sanchez *et al.* (SANCHEZ *et al.*, 2021)	2021	Propõe uma abordagem para a seleção de características estatísticas para a detecção de ataques DDoS usando aprendizado profundo.
Srihari e Anitha (SRIHARI; ANITHA, 2014)	2014	Propõe um sistema de detecção de ataques DDoS usando *wavelets* e aprendizado semi-supervisionado.
Kim e Kim (KIM; KIM; LEE, 2013)	2013	Propôs um algoritmo ativo distribuído, fundamentado em propriedades do invasor, que correlaciona fluxos de tráfego diversos na rede para identificar ataques DDoS.
Marciel *et al.* (MACIEL *et al.*, 2018)	2018	Apresenta uma introdução de um modelo hierárquico para descrever o comportamento dos elementos de um sistema durante um ataque DDoS (Distributed Denial of Service).
Nagy *et al.* (NAGY *et al.*, 2018)	2018	Propuseram um detector de ataques DDoS de alta velocidade utilizando FPGA.
Shorey *et al.* (SHOREY *et al.*, 2018)	2018	Apresenta uma análise comparativa de padrões de tráfego gerado por ferramentas de ataques DDoS populares.
Este trabalho	2024	Um panorama atualizado sobre uma análise comparativa do fluxo de tráfego gerado por ferramentas de ataque DDoS.

A segurança da Internet demanda medidas e contramedidas eficazes contra ataques DoS/DDoS, dada a sua ameaça em larga escala em grandes redes. Tais abordagens precisam ser adaptáveis para serem aplicadas em diferentes camadas e níveis da infraestrutura. Diversos esforços foram realizados para integrar dados provenientes de diversas ferramentas de ataque DoS/DDoS (WHITMAN; MATTORD, 2016).

No trabalho proposto por Chahal et al. (CHAHAL; KAUR; SHARMA, 2021) fornece uma visão abrangente dos desafios e soluções para a defesa contra ataques DDoS em ambientes SDN. Os autores apresentam uma taxonomia de mecanismos de defesa contra DDoS em ambientes SDN que é útil para a compreensão dos diferentes tipos de mecanismos disponíveis.

Sanchez et al. (SANCHEZ et al., 2021) propõe uma abordagem para a seleção de características estatísticas para a detecção de ataques DDoS usando aprendizado profundo visando reduzir o número de características necessárias para a detecção de ataques DDoS, sem reduzir significativamente a precisão da detecção. A abordagem proposta é baseada em uma análise de variância (ANOVA), que é usada para identificar as características estatísticas mais importantes para a detecção de ataques DDoS. Uma vez identificadas as características mais importantes, é utilizado um algoritmo de aprendizado profundo para treinar um modelo de detecção de ataques DDoS.

Srihari e Anitha (SRIHARI; ANITHA, 2014) propõe um sistema de detecção de ataques DDoS usando wavelets e aprendizado semi-supervisionado, tendo eficiência em termos de recursos e é capaz de detectar ataques DDoS de diferentes tipo. O sistema é baseado na identificação de padrões característicos de ataques DDoS em séries temporais de tráfego de rede.

Kim e Kim (KIM; KIM; LEE, 2013) propuseram um algoritmo ativo distribuído, fundamentado em propriedades do invasor, que correlaciona fluxos de tráfego diversos na rede para identificar ataques DDoS. Uma das vantagens desse algoritmo é a sua independência de regras de filtragem específicas, tornando-o apto para detectar uma ampla gama de ataques DDoS genéricos.

Marciel et al. (MACIEL et al., 2018) introduziram um modelo hierárquico destinado a descrever o comportamento dos elementos do sistema durante um ataque DDoS. Este modelo avalia a praticabilidade, vantagem e probabilidade de ataque a esses elementos. A árvore de ataque pode indicar a severidade dos ataques simultâneos em relação à disponibilidade do sistema alvo.

Nagy et al. (NAGY et al., 2018) propuseram um detector de ataques DDoS de alta velocidade utilizando FPGA. Afirma-se que esse detector é capaz de identificar os principais tipos de ataques DDoS, incluindo a maioria dos ataques "hit and run", em questão de milissegundos.

No trabalho proposto por Shorey et al. (SHOREY et al., 2018) forneceu uma análise comparativa de padrões de tráfego gerado por ferramentas de ataques DDoS populares, visando detectar técnicas de proteção DDoS de maneira eficaz comparando três ferramentas de ataque DDoS.

Os métodos de defesa DoS/DDoS mencionados acima têm sua fundação no comportamento e nas características dos invasores. Assim, a investigação e análise dos padrões e procedimentos adotados pelo atacante trazem uma contribuição valiosa para o desenvolvimento eficaz de estratégias de defesa.

Este estudo apresenta semelhanças com a pesquisa conduzida por (SHOREY et al., 2018), a qual realizou uma análise comparativa envolvendo três ferramentas distintas para DoS/DDoS. No entanto, difere desse trabalho ao incorporar uma ferramenta adicional de ataque, resultando em um panorama atualizado para o desenvolvimento de contramedidas. Este artigo objetiva-se fornecer uma análise comparativa do fluxo de tráfego gerado por ferramentas de ataque DoS/DDoS amplamente utilizadas, realizando um comparativo entre quatro dessas ferramentas. Desta maneira, buscando oferecer uma visão atualizada das ferramentas DoS/DDoS, o que representa um diferencial significativo para a compreensão do panorama atual desse cenário.

2 REFERENCIAL TEÓRICO

Esta Seção apresenta conceitos relevantes para a compreensão deste trabalho.

2.1 SEGURANÇA DA INFORMAÇÃO

A segurança da informação desempenha um papel vital na proteção dos sistemas e dados de uma organização contra ameaças, como os ataques DoS e DDoS. Estes últimos, em particular, representam uma ameaça significativa, podendo resultar em graves consequências para a organização (DUO; ZHOU; ABUSORRAH, 2022). Além de comprometerem a disponibilidade dos serviços online, os ataques DoS/DDoS podem levar à perda de dados sensíveis, causar interrupções operacionais, danificar a reputação da empresa e resultar em impactos financeiros significativos. A indisponibilidade dos serviços online de uma organização devido a um ataque bem-sucedido não apenas afeta a experiência do usuário, mas também pode levar à perda de confiança por parte dos clientes. A incapacidade de acessar sistemas ou realizar transações online pode resultar em danos financeiros imediatos e afetar a continuidade dos negócios. Além disso, a exposição a um ataque DoS/DDoS bem-sucedido pode resultar na perda ou comprometimento de dados confidenciais, levando a implicações legais, regulatórias e de conformidade, ampliando ainda mais o impacto negativo sobre a organização (WHITMAN; MATTORD, 2016).

2.2 APLICABILIDADE DAS LEIS DE ATAQUES CIBERNÉTICOS NO BRASIL

As legislações brasileiras referentes aos ataques cibernéticos, incluindo os casos de ataques DoS e DDoS, são aplicadas de forma casuística, levando em consideração as circunstâncias particulares de cada ocorrência. De forma geral, a tipificação de um ataque DoS/DDoS como crime requer a constatação de danos efetivos, tais como a interrupção do funcionamento de um sistema ou site. A Lei 12.737/2012 (BRASIL, 2012), popularmente conhecida como "Lei Carolina Dieckmann", pode ser aplicada para punir ataques DoS/DDoS que causem interrupção de serviço telemático ou de informação de utilidade pública. Contudo, para que essa legislação seja aplicada, é imprescindível que o ataque resulte em danos concretos, como a paralisação operacional de um sistema ou site. O Código Penal Brasileiro (Decreto-Lei 2.848/1940) (BRASIL, 1940), também pode ser aplicado para punir ataques DoS/DDoS. O artigo 163 do Código Penal, por exemplo, tipifica o crime de dano qualificado, que é a conduta de "destruir, inutilizar ou deteriorar coisa alheia". Se um ataque DoS/DDoS causar danos a um sistema ou rede, o responsável pelo ataque pode ser condenado por crime de dano qualificado. Além da Lei 12.737/2012 e do Código Penal Brasileiro, outras leis também podem ser aplicadas para punir ataques DoS/DDoS. Por exemplo, a Lei 12.965/2014 (BRASIL, 2014), popularmente conhecida como "Marco Civil da Internet", prevê que o usuário deve se abster de "violar a inviolabilidade do sigilo das comunicações". Se um ataque DoS/DDoS for realizado para obter dados pessoais ou sigilosos de uma vítima, o responsável pelo ataque pode ser condenado por crime de violação de sigilo.

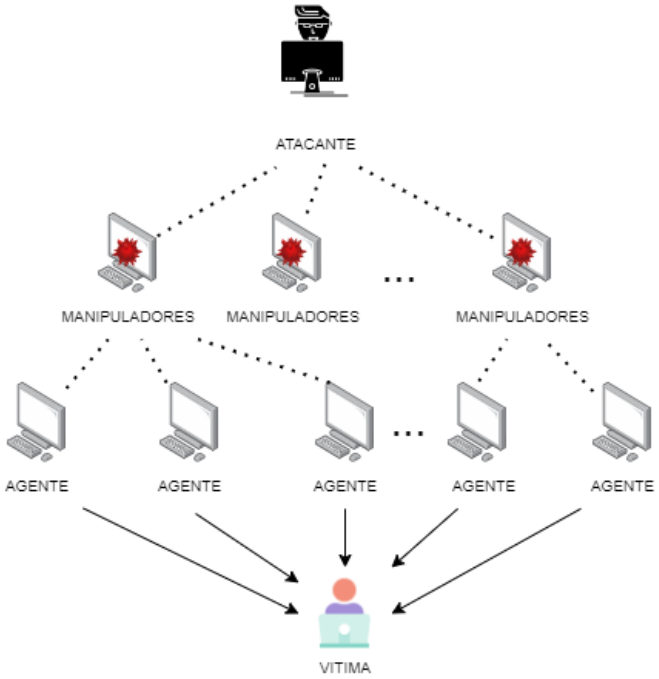
2.3 ATAQUES DE NEGAÇÃO DE SERVIÇO (DOS) E DE NEGAÇÃO DE SERVIÇO DISTRIBUÍDOS (DDOS)

Os ataques DoS e DDoS são técnicas utilizadas por atacantes para sobrecarregar um servidor ou rede, tornando-o indisponível para os usuários legítimos. Esses ataques pode ser considerados uma das principais ameaças à segurança da informação, uma vez que podem causar indisponibilidade dos serviços online e perdas financeiras significativas para empresas (DOULIGERIS; MITROKOTSA, 2017). Os ataques DoS geralmente envolvem o uso de um único computador ou dispositivo para enviar um grande volume de tráfego para o servidor alvo. Já os ataques DDoS envolvem o uso de múltiplos dispositivos, muitas vezes pertencentes a uma botnet[3], para enviar tráfego para o servidor alvo (HOQUE; BHATTACHARYYA; KALITA, 2015). Os ataques DDoS são geralmente mais efetivos do que os ataques DoS, já que envolvem um grande número de dispositivos, dificultando a detecção e mitigação dos ataques (BARANI; SINGH, 2021).

A figura 1 apresenta a arquitetura de um ataque DDoS.

[3] https://www.hardware.com.br/artigos/o-que-e-uma-botnet/

Figura 1 - Arquitetura de ataque DDoS



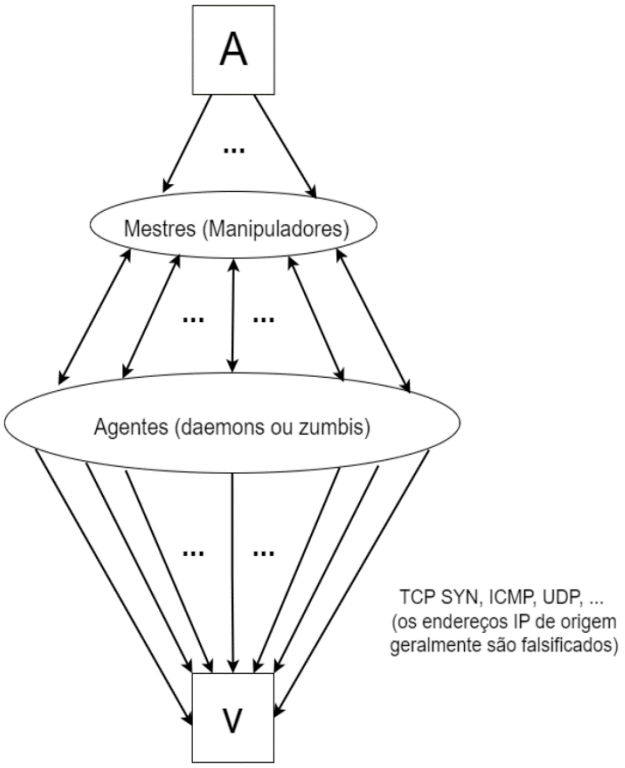
2.3.1 Tipos de Ataques DDoS

Os ataques DDoS são geralmente classificados em duas categorias distintas: ataques diretos e ataques refletores. Nos ataques diretos, os hosts comprometidos lançam diretamente o ataque contra o alvo. Por outro lado, nos ataques refletores, os hosts comprometidos enviam pacotes de solicitação com endereços IP falsificados, resultando na presença do IP da máquina alvo no campo de endereço de origem dos pacotes IP (NAGPAL et al., 2015). Essa técnica visa dificultar a identificação do verdadeiro ponto de origem do ataque, tornando a defesa contra tais ataques mais desafiadora.

I. Ataques Diretos

Em um ataque direto, a vítima é inundada por um elevado volume de pacotes enviados diretamente pelo agressor, como ilustrado na Figura 2. Estes pacotes de ataque podem ser do tipo TCP, ICMP, UDP ou uma combinação destes. Diversos métodos são empregados para executar o ataque, entre eles o SYN Flooding, RST Flooding e ICMP Flooding. Cada um desses métodos visa explorar diferentes vulnerabilidades e protocolos, amplificando o impacto do ataque sobre o alvo.

Figura 2 - Arquitetura de ataque direto

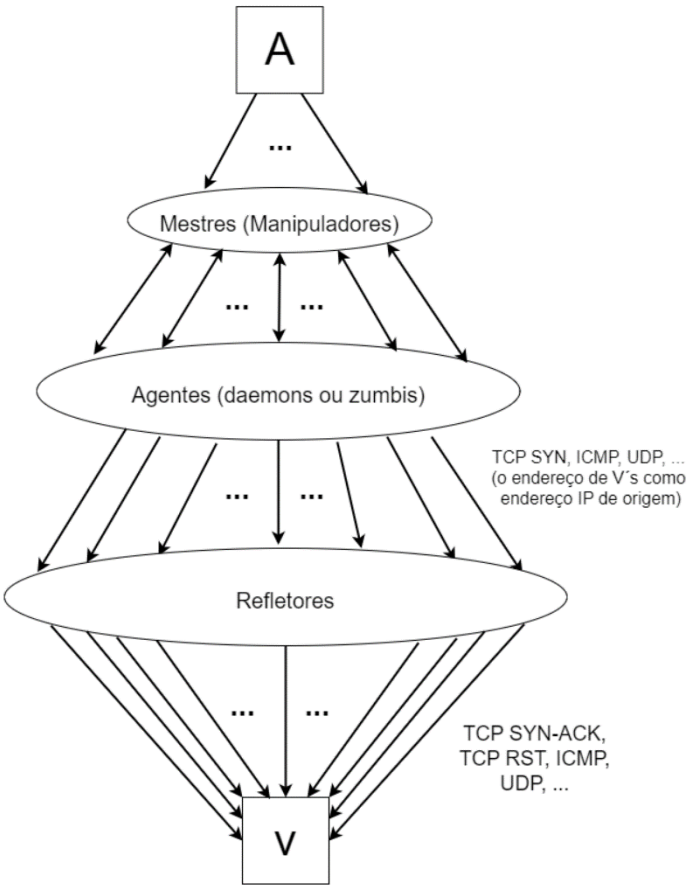


Outro aspecto crucial é o rastreamento de IP, que consiste na identificação do remetente original do pacote na Internet, independentemente dos detalhes específicos de sua origem. Enquanto o rastreamento de IP é viável em ataques diretos, torna-se uma tarefa desafiadora quando um ataque DoS/DDoS está em curso. Geralmente, essa identificação só é possível após a execução do ataque (PATIL; PAWALE, 2014).

II. Ataques de Refletores

Os ataques de reflexão são realizados por meio de roteadores que desempenham o papel de intermediários, denominados 'refletores'. Estes refletores são intencionalmente configurados para agir como vetores de ataque, conforme esquematizado na Figura 3. Embora os métodos empregados nos ataques diretos possam ser utilizados nos ataques de reflexão, a estratégia é distintamente diferenciada. Esses refletores são explorados para redirecionar e amplificar o tráfego malicioso, muitas vezes usando protocolos legítimos, mas manipulados de forma a gerar respostas em massa a partir de sistemas alvos. Esta abordagem visa a sobrecarga dos recursos desses sistemas alvos por meio da amplificação do volume de tráfego recebido, comparativamente ao tráfego inicialmente enviado pelo atacante.

Figura 3 - Arquitetura de ataque refletor



2.3.2 Ferramentas de Ataque DoS/DDoS e sua Classificação

Diversas ferramentas estão disponíveis para realizar ataques de DoS/DDoS. O *Slowloris*, por exemplo, é uma ferramenta eficaz que funciona abrindo inúmeras conexões com o servidor web direcionado e mantendo-as abertas por um período de tempo indefinido (BUKAC; MATYAS, 2015; ZARGAR; JOSHI; TIPPER, 2013). Usando essas conexões, ele transfere solicitações HTTP fracionárias de forma ininterrupta. Como resultado, os servidores sob ataque mantêm as conexões abertas, enquanto aguardam que as solicitações de ataque fracionário sejam concluídas. Uma aplicação mais recente comparada ao *Slowloris* é o *GoldenEye* (BRAVO; MAURICIO, 2018). É uma aplicação *python* apenas para fins de teste de segurança. Quando usado para fins maliciosos, é capaz de derrubar os servidores web de suas vítimas. O *Xerxes*, desenvolvido em 2017, é uma das mais recentes e poderosas ferramentas DDOS (BADOTRA; PANDA, 2021). É desenvolvido em C e portanto requer uma fase de compilação. Ele usa a porta número 80 para atacar a web, resultando no bloqueio das respostas da web à medida que a conexão entre o servidor e o cliente deixa de existir. A ferramenta *Torshammer*, uma aplicação em *python*, é conhecido por ser um dos ataques mais eficazes em termos de saturação da largura de banda. Ela trabalha através da utilização da rede Tor para realizar ataques DDoS, tornando a origem do ataque mais difícil de rastrear (WANI et al., 2019; FADHLILLAH; KARNA; IRAWAN, 2021).

I. Interface

A interface de uma ferramenta atacante DoS/DDoS pode ser baseada no clássico interpretador de linha de comando (CLI) ou em uma interface gráfica de usuário (GUI). O *GoldenEye*, por exemplo, é uma ferramenta que utiliza uma interface de linha de comando (CLI), oferecendo um conjunto de opções e comandos para configurar e executar os ataques (SHOREY et al., 2018). Em contrapartida, ferramentas como o *XOIC* possuem uma interface gráfica de usuário (GUI), que proporciona uma experiência mais visual e intuitiva para operar o programa. Assim como o *GoldenEye* e o *XOIC*, o *Torshammer* representa uma opção poderosa em termos de ferramentas de ataque DDoS, oferecendo diferentes abordagens e recursos para realização de testes de segurança e avaliação de resiliência de sistemas.

II. Dinâmica da Taxa de Ataque

A detecção dos ataques pode ser facilitada quando os pacotes são enviados de maneira contínua a uma taxa constante pelo invasor. Por esse motivo, a adoção de uma taxa variável se torna preferível, pois confere maior cautela ao envio dos pacotes. Essa variabilidade na taxa de envio pode seguir uma dinâmica que permite um aumento gradual ao longo do tempo ou variações com flutuações ao longo do período do ataque. A estratégia de empregar uma taxa de envio variável oferece vantagens em termos de dissimulação do ataque, dificultando a detecção imediata por parte da vítima. Ao alterar a dinâmica de envio, seja aumentando gradualmente ou variando as taxas, o atacante busca evadir a detecção automatizada e tornar a resposta da vítima mais desafiadora, exigindo uma adaptação constante às mudanças na intensidade do ataque.

III. Categoria de Ataque ou Base de Vulnerabilidade

Existem dois tipos de DDoS com base no tipo de alvo do ataque: i) Ataque de Exaustão de Largura de Banda e ii) Ataque de Exaustão de Recursos. No Ataque de Exaustão de Largura de Banda, o atacante sobrecarrega o endereço IP ao enviar grandes volumes de tráfego. Isso leva o sistema alvo a operar de forma muito lenta, travar ou ficar em um estado de sobrecarga de largura de banda, resultando na indisponibilidade para usuários legítimos. Exemplos desses ataques incluem TCP SYN e PUSH+ACK. Já no Ataque de Exaustão de Recursos, pacotes maliciosos são enviados para interromper e abusar das comunicações do protocolo de rede. Isso acaba por bloquear e distorcer os recursos da rede.

IV. Arquitetura do Modelo de Ataque

Existem dois modelos arquiteturais de DDoS: o modelo de agente manipulador e o modelo refletor. No modelo de agente manipulador, os manipuladores são pacotes de software implantados na Internet e utilizados pelo invasor para iniciar o ataque. O invasor regularmente obtém informações sobre os agentes ativos e em execução, visando interromper a comunicação e o equilíbrio de carga desses agentes. No modelo refletor, os manipuladores exercem controle sobre o agente. Como resultado, o invasor falsifica o endereço IP do manipulador e sobrecarrega o agente, inundando o endereço IP da vítima com pacotes. No modelo baseado em IRC, estabelece-se um canal público de comunicação de retransmissão na Internet entre o cliente e o agente para conduzir os ataques.

V. Protocolo

Os ataques de inundação constituem o tipo principal dessa categoria. Eles envolvem o envio de um fluxo contínuo de solicitações SYN para obstruir e esgotar a rede da vítima, resultando na incapacidade de resposta para os usuários legítimos. Existem diversos tipos de ataques de inundação, como os ataques de inundação HTTP, TCP, UDP e ICMP.

VI. Área Alvo

Em uma rede, um invasor possui a capacidade de executar um ataque direcionado aos links ou aos terminais. Os terminais, normalmente associados ao servidor da vítima, são alvos específicos que implicam um ataque direto ao servidor em si ou à totalidade da rede. Os terminais dentro da rede frequentemente referem-se aos pontos finais, como servidores, nos quais o atacante concentra seus esforços. Esse direcionamento específico implica uma estratégia focalizada,

visando comprometer diretamente um servidor específico ou afetar a funcionalidade e a integridade da rede como um todo

3 METODOLOGIA

Esta seção apresenta a metodologia empregada neste artigo, na qual mostra como o estudo foi planejado e executado e quais estratégias foram utilizadas.

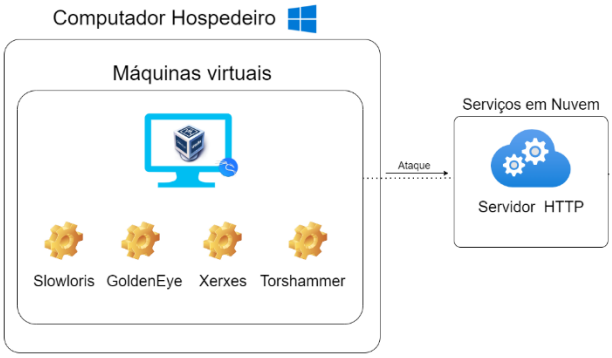
3.1 DESIGN EXPERIMENTAL

Para a realização deste artigo, avaliou-se o desempenho das ferramentas *Slowloris*, *GoldenEyes*, *Xerxes* e *Torshammer* em um ambiente simulado. A seleção dessas ferramentas foi baseada na diversidade de técnicas que oferecem para ataques DoS/DDoS. O *Slowloris* destaca-se pela eficiência singular em derrubar servidores com baixa largura de banda. *GoldenEyes*, *Xerxes* e *Torshammer* foram escolhidos pela variedade de abordagens, incluindo ataques distribuídos e saturação de recursos. A escolha visa replicar cenários do mundo real, onde diferentes métodos são adotados por atacantes, garantindo uma análise abrangente do impacto potencial dos ataques simulados.

Utilizando a seguinte especificação da maquina: *Windows* 11 Pro 64 bits, processador *Intel core* i3 8th Gen, memória RAM de *8GB* e armazenamento *SSD NVMe M.2* de *250GB*. Empregou-se máquinas virtuais nas seguintes configurações: Sistema operacional *Kali Linux versão 2023.2*, com 2 processadores, memória RAM de *2GB* e armazenamento de *80GB*. O objetivo é executar um ataque de negação de serviço (DoS) direcionado a um website convencional, denominado **www.testeddos.shop**. Este website foi especificamente desenvolvido para servir como parte integrante deste projeto de pesquisa. Ele incorpora configurações iniciais e configurações típicas de um site que não apresenta sistemas avançados de proteção contra ataques cibernéticos, empregando as ferramentas identificadas e ilustradas na figura 4. Antes disso, foi conduzido um estudo sobre a natureza do fluxo de rede em cada um dos casos, utilizando uma aplicação de monitoramento de rede gráfico chamada *EtherApe*[4] . Esta aplicação exibe as atividades nos modos de camada de Link, IP e TCP, além de oferecer uma interface gráfica para visualizar as atividades de rede. O tamanho do host e do link é dinâmico e altera de acordo com o tráfego atual. Os protocolos são codificados por cores para facilitar a visualização, incluindo Ethernet, FDDI, Token Ring, ISDN, PPP, SLIP e dispositivos WLAN, bem como vários formatos de encapsulamento. O *EtherApe* também oferece suporte para a filtragem de tráfego a partir de dados em tempo real ou de registros de tráfego armazenados. O status de atividade/inatividade do site é verificado em ***www.hostinger.com.br*** provedor de Hospedagem Web utilizado no site. A escolha da *Hostinger* como provedor de hospedagem para o website alvo, ***www.testeddos.shop***, baseou-se em diversos critérios estratégicos. Ela é conhecida por oferecer uma ampla gama de serviços de hospedagem web, sendo amplamente utilizada por empresas e desenvolvedores.

[4] https://etherape.sourceforge.io/

Figura 4 - Design Experimental



3.2 ATAQUE UTILIZANDO *SLOWLORIS*

A concepção do software de ataque DoS/DDoS conhecido como *Slowloris* foi atribuída a Robert “RSnake” Hansen. Sua notável eficácia reside na capacidade de derrubar um servidor web com apenas um computador (ZARGAR; JOSHI; TIPPER, 2013). O destaque deste programa está na sua capacidade singular de mirar especificamente um alvo predefinido, sem interferir com outros serviços ou portas, mostrando uma abordagem direcionada e precisa em suas ações. Esta ferramenta requer pouca ou nenhuma largura de banda para a execução de seus ataques (BUKAC; MATYAS, 2015). A nomenclatura "Slowloris"origina-se da capacidade peculiar deste artefato em consumir os recursos HTTP de um servidor de forma gradual e perspicaz. Destaca-se, porém, que se trata de uma ferramenta DoS/DDoS direcionada ao protocolo HTTP, não devendo ser confundida com uma aplicação voltada ao protocolo TCP. No cerne de seu funcionamento, encontra-se o estabelecimento de uma conexão TCP legítima com o host de destino, seguido de uma inundação calculada com múltiplas conexões HTTP parciais. Estas conexões parciais são mantidas propositadamente abertas pelo maior lapso temporal viável, sendo remetidas de maneira ininterrupta, almejando a exaustão dos recursos do alvo (SABRI; ISMAIL; HAZZIM, 2021). Tal estratégia outorga ao agressor a habilidade de transitar com êxito através de sistemas de prevenção de intrusões, uma vez que não se faz necessário o envio de pacotes malformados.

A limitação do *Slowloris* reside no fato de que os servidores web da atualidade estão equipados com recursos robustos para atenuar um eventual ataque desse tipo. Entre essas tecnologias, destacam-se:

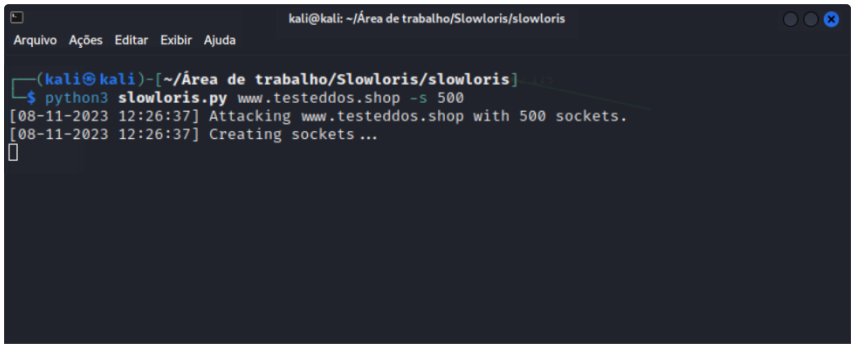
1. Ampliando a capacidade de atendimento a um número maior de clientes que o servidor web terá a capacidade de suportar;
2. Limitando o número de conexões que um único endereço IP pode estabelecer;
3. Impondo restrições quanto à menor velocidade de transferência que uma conexão está autorizada a ter;
4. Estabelecendo um limite de tempo para a permanência de cada cliente conectado;

No *Slowloris*, foi incorporado um cronômetro no código-fonte responsável pela construção dos soquetes. Tal medida auxilia no cálculo do tempo requerido para estabelecer um soquete com êxito. Em cenários ideais, apenas um soquete se mostra suficiente para comprometer um site. Assim, a média das discrepâncias temporais fornece o intervalo necessário para a execução bem-sucedida de um ataque que resulte na queda de um site.

Ao utilizar a ferramenta *Slowloris*, disponível no *Github*[5], é necessário inserir o seguinte comando no terminal: *'python3 slowloris.py'*, indicando que se trata de um arquivo *python*. Em seguida, é preciso fornecer o nome do host ou o endereço IP do alvo, seguido da opção *'-s'*, que representa o número de sockets a serem enviados. No exemplo mencionado, esse número é especificado como '500', como mostra na figura 5.

O número de sockets desempenha um papel crucial na dinâmica do ataque. Ao aumentar esse numero, o atacante intensifica a pressão exercida sobre o servidor-alvo. Esse aumento resulta em mais conexões simultâneas sendo estabelecidas, o que pode sobrecarregar a capacidade do servidor de lidar com essas conexões. Cada socket estabelecido consome recursos do servidor, como portas disponíveis, memória e capacidade de processamento.

Figura 5 - Ferramenta Slowloris Atacando



3.3 ATAQUE UTILIZANDO *GOLDENEYE*

O *GoldenEye* é uma ferramenta desenvolvido usando *python*, especializada em testes de negação de serviço (DoS) voltada para camadas HTTP/S Layer 7. Utilizando a técnica KeepAlive em conjunto com configurações de Cache-Control, o *GoldenEye* busca prolongar a exploração da conexão do soquete através do cache, visando consumir todos os soquetes disponíveis no servidor HTTP/S (KSHIRSAGAR; SHAIKH, 2019). Esta ferramenta é altamente competente e amplamente recomendada para a análise de ambientes focados em malware. Ele pode capturar proativamente as peculiaridades delicadas da condição do malware na execução de última geração e selecionar as configurações mais prováveis. Além disso, possui a habilidade de adaptar dinamicamente a sua estrutura online para otimizar o processo de análise. Essa ferramenta demonstra uma eficácia notável ao identificar o ambiente alvo do malware, utilizando um mecanismo de execução especulativa desenvolvido para monitorar as práticas de malware em circunstâncias diversas e variáveis.

O *GoldenEye*, ao evoluir de maneira adaptativa, tem a capacidade de modificar o ambiente, conduzindo a uma análise que possibilita ao próprio malware revelar seus objetivos, alvos e contexto (SHOREY et al., 2018). Vale ressaltar que, embora o *GoldenEye* demande recursos significativos para operar em alta velocidade, a observação prática revelou sua exigência por hardware de alta capacidade, devido ao uso intensivo de memória, mantendo, contudo, uma eficiência notável. A função de timer é implementada na ferramenta de forma que o código-fonte seja independente do ambiente do sistema operacional.

Ao utilizar a ferramenta *GoldenEye*, disponível no *Github*[6], é necessário inserir o seguinte comando no terminal: *'python3 goldeneye.py'*, indicando que se trata de um arquivo *Python*. Em seguida, é preciso fornecer o nome do host ou o endereço IP do alvo, seguido da opção *'-s'*, que

[5] https://github.com/gkbrk/slowloris
[6] https://github.com/jseidl/GoldenEye

representa o número de *sockets* a serem enviados. No exemplo mencionado, esse número é especificado como ’500’, como mostra na figura 6.

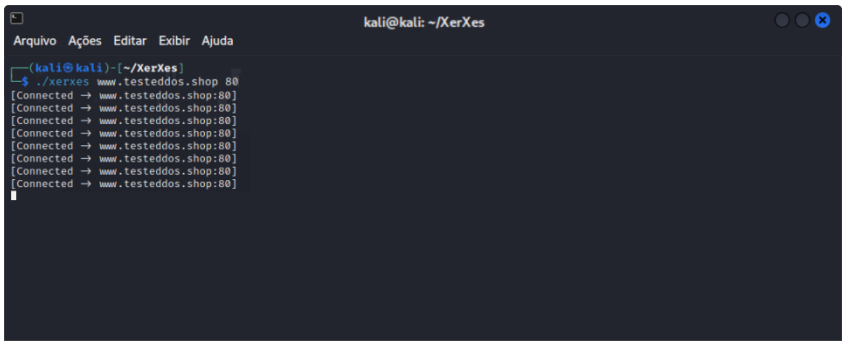
Figura 6 - Ferramenta GoldenEye Atacando

3.4 ATAQUE UTILIZANDO *XERXES*

O *Xerxes* é uma ferramenta de ataque DoS/DDoS desenvolvida pelo hacker ‘The Jester’ em 2017 sendo a mais recente criada pelo mesmo. Ao contrário dos ataques DDoS tradicionais que utilizam vários servidores, o *Xerxes* explora uma vulnerabilidade no Apache HTTP, enviando pacotes malformados que o servidor leva vários segundos para processar, mas apenas uma fração de segundo para serem enviados (BADOTRA; PANDA, 2021). Ao disparar centenas desses pacotes por segundo, o *Xerxes* é capaz de sobrecarregar o Apache e derrubar o servidor. Este tipo de ataque difere dos DDoS convencionais, pois não se baseia na obstrução dos canais que levam ao servidor, mas sim na sobrecarga direta do servidor web. Portanto, a quantidade de largura de banda disponível no servidor torna-se irrelevante. Mesmo se um novo servidor for adicionado, ele apenas aumentará o tráfego em n+1, tornando-o ainda mais vulnerável a ser desativado.

Ao utilizar a ferramenta *Xerxes*, disponível no *Github*[7], é necessário inserir o seguinte comando no terminal: *‘./xerxes’*, indicando um arquivo escrito em *linguagem C*. Em seguida, é necessário fornecer o nome do host ou o endereço IP do alvo, seguido pela especificação da porta à qual o ataque será direcionado. No exemplo mencionado, essa porta é identificada pelo número ’80’, como mostra na figura 7.

Figura 7 - Ferramenta Xerxes Atacando



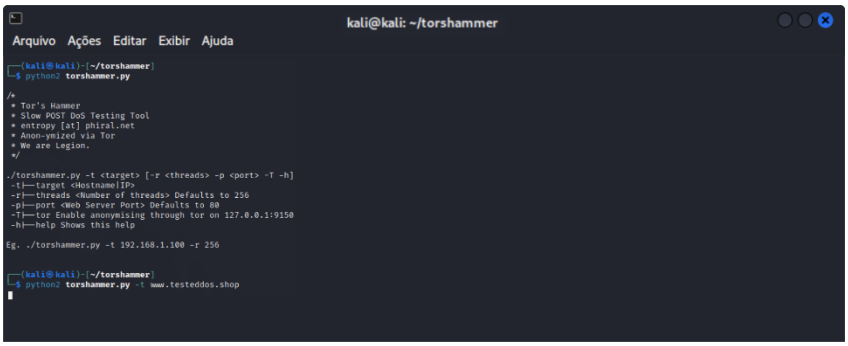
3.5 ATAQUE UTILIZANDO *TORSHAMMER*

[7] https://github.com/CyberXCodder/XerXes

Embora tenha sido desenvolvido em 2009, o *Torshammer* continua sendo uma ferramenta amplamente utilizada nos dias de hoje. É uma ferramenta pós-HTTP, escrita em Python, notória por sua alta eficiência e seu impacto nos servido res Apache. Ao contrário dos ataques DoS/DDoS convencionais, que visam sobrecarregar os servidores-alvo com tráfego proveniente de várias fontes, o Torshammer concentra-se em um servidor Tor específico (FADHLILLAH; KARNA; IRAWAN, 2021). O '*modus operandi'* do *Torshammer* envolve o envio de uma grande quantidade de requisições HTTP ao servidor, sendo cada uma delas meticulosamente elaborada para consumir uma quantidade significativa de recursos de processamento. Esta abordagem lenta de pós-DoS resulta no esgotamento gradual dos recursos do alvo, gerando um elevado número de conexões HTTP POST por um período prolongado, que pode durar de 1.000 a 30.000 segundos (WANI et al., 2019). Essa persistência no uso desta ferramenta destaca a sua relevância contínua como uma ferramenta de ataque capaz de causar danos consideráveis aos servidores específicos.

Ao utilizar a ferramenta *Torshammer*, disponível no *Github*[8], é necessário inserir o seguinte comando no terminal: '*python2 torshammer.py'*, indicando que se trata de um arquivo python. Em seguida, é preciso inserir a opção *'-t*', seguido o nome do host ou o endereço IP do alvo. No exemplo mencionado, as configurações de ataque foram mantidas por padrão, como mostra na figura 8.

Figura 8 - Ferramenta Torshammer Atacando



A Tabela 2 apresenta uma síntese e comparação das características comuns entre as ferramentas *Slowloris*, *GoldenEye*, *Xerxes* e *Torshammer*. Os parâmetros analisados incluem a natureza do alvo, os sistemas operacionais suportados, a interface utilizada e se proporcionam a funcionalidade de mascaramento de IP (IP Spoofing).

Tabela 2 - Comparação de características comuns

Ferramenta	Ano	Implementação	Alvo		Sistema Operacional			Interface		IP Sp.
			Band.	Res.	Win.	Linux	MAC	CLI	GUI	
Slowloris	2009	Perl					-			Não
GoldenEye	2012	Python	-						-	Não
Xerxes	2017	C					-		-	Não
Torshammer	2009	Python			-				-	Não

Band. = Bandwidth; Res. = Resource; Win. = Windows; Sp = Spoofing;

4 EXPERIMENTOS E RESULTADOS

Nesta seção, serão apresentados os resultados da pesquisa.

[8] https://github.com/Karlheinzniebuhr/torshammer

As características de tráfego dos ataques DoS/DDoS empregando as ferramentas *Slowloris*, *GoldenEye*, *Xerxes* e *Torshammer* foram analisados e apresentados nas tabelas 3, 4, 5 e 6, respectivamente. Estes estudos experimentais foram conduzidos em um ambiente controlado, mantendo-se o intervalo de duração dos ataques entre 10 e 15 minutos, com a configuração básica adotada para este projeto. A ferramenta *EtherApe* foi empregado na coleta abrangente de informações referentes ao tráfego instantâneo, tráfego acumulado, tamanho das mensagens e portas utilizadas.

De acordo com a Tabela 3, o ***Slowloris*** direciona a maior parte do seu tráfego para o protocolo HTTP, evidenciado por uma taxa instantânea significativa de 191,36 Kbps. Essa intensidade aponta para um ataque vigoroso, visando explorar vulnerabilidades específicas no protocolo. O tráfego acumulado atinge 5,74 Mb no protocolo HTTP, revelando uma estratégia eficaz em sobrecarregar o servidor-alvo. A quantidade substancial de dados transmitidos destaca a capacidade do Slowloris de provocar uma sobrecarga significativa.

Embora o tráfego no protocolo HTTPS seja notavelmente inferior em comparação com o HTTP, a sua utilização sugere uma tentativa de diversificar os métodos de ataque. A taxa instantânea de 1,50 Kbps, no entanto, indica uma abordagem mais moderada nesse contexto. Outros protocolos, como DNS, apresentam uma taxa instantânea significativa, mas o tráfego acumulado é relativamente menor. Isso sugere que o Slowloris concentra seus esforços principalmente no protocolo HTTP, mantendo, ao mesmo tempo, uma presença moderada em outros protocolos.

Os protocolos ICMPv6, IGMP, mDNS e NTP não demonstram atividade significativa, indicando que o Slowloris não prioriza esses protocolos em sua abordagem de ataque.

Tabela 3 - Análise instantânea das características de ataque do Slowloris

Protocolo	Taxa de tráfego instantâneo	Tráfego acumulado	Tam. da mensagem (Bytes)	Porta
DNS	66,38Kbps	1,48 Mb	100 bytes	53
HTTP	191,36Kbps	5,74 Mb	162 bytes	80
HTTPS	1,50Kbps	680,82 Kb	277 bytes	443
ICMPV6	0bps	2,73 Kb	34 bytes	-
IGMP	0bps	34 Kb	90 bytes	-
MDNS	0bps	24 Kb	147 bytes	5353
NTP	0bps	363,90 Kb	116 bytes	123

Quanto ao ***GoldenEye***, conforme a Tabela 4, a ferramenta concentra sua atividade no protocolo HTTP, evidenciada por uma taxa instantânea significativa de 185,36 Kbps. Esse destaque sugere uma estratégia focada em explorar vulnerabilidades específicas desse protocolo. Além disso, a ferramenta demonstra uma ênfase adicional no protocolo HTTPS, apresentando um tráfego acumulado de 8,90 Mb. Essa abordagem indica uma tentativa de explorar possíveis vulnerabilidades no tráfego seguro da web.

O *GoldenEye* mantém uma presença significativa no protocolo DNS, com uma taxa instantânea de 29,71 Kbps. No entanto, o tráfego acumulado é relativamente menor, sugerindo uma exploração moderada desse protocolo. Outros protocolos, como ICMPv6, mDNS e NTP, mostram atividade mínima ou nula, indicando que o GoldenEye prioriza o protocolo HTTP, com alguma atenção adicional ao HTTPS e DNS.

A presença de tráfego em um "IP UNKNOWN"sugere que o *GoldenEye* pode estar explorando protocolos não identificados. Embora a taxa e o tráfego acumulado sejam baixos, a natureza desconhecida demanda atenção e destaca a possibilidade de exploração de serviços não claramente identificados.

Tabela 4 - Análise instantânea das características de ataque do GoldenEye

Protocolo	Taxa de tráfego instantâneo	Tráfego acumulado	Tam. da mensagem (Bytes)	Porta
DNS	29,71Kbps	933,88 Kb	91 bytes	53
HTTP	185,36Kbps	4,14 Mb	201 bytes	80
HTTPS	18,06Kbps	8,90 Mb	583 bytes	443
ICMPV6	0bps	1,01 Kb	113 bytes	-
MDNS	0bps	1,09 Kb	131 bytes	5353
NTP	0bps	526 bytes	105 bytes	123
IP UNKNOWN	0bps	414 bytes	127 bytes	-

Conforme os dados apresentados na Tabela 5, o ***Xerxes*** direciona sua atividade predominantemente para o protocolo HTTP e DNS, já que o HTTP usa DNS para resolução de endereços, exibindo uma taxa instantânea considerável de 24,75 Kbps e 7,91 Kbps respectivamente. Além disso, acumula uma quantidade significativa de tráfego no protocolo HTTP, totalizando 2,59 Mb. Já no protocolo DNS, totalizando 3,55 Mb. Essa abordagem destaca a tentativa de sobrecarregar o servidor web por meio de solicitações HTTP, evidenciando a estratégia de gerar uma carga substancial nesse protocolo.

A ferramenta também demonstra atividade no protocolo HTTPS, com uma taxa instantânea de 12,24 Kbps. Apesar de menos proeminente em comparação com o HTTP, a acumulação de tráfego HTTPS de 126,91 Kb indica uma exploração adicional desse protocolo.

Protocolos como ICMPv6, mDNS e NTP exibem atividade mínima ou nula, indicando que o *Xerxes* prioriza o protocolo HTTP, com alguma atenção ao HTTPS. Assim como o *GoldenEye*, o *Xerxes* também apresenta tráfego em um "IP UNKNOWN". Embora a taxa e o tráfego acumulado sejam baixos, a natureza desconhecida sugere a possibilidade de exploração de protocolos não identificados.

Tabela 5 -Análise instantânea das características de ataque do Xerxes

Protocolo	Taxa de tráfego instantâneo	Tráfego acumulado	Tam. da mensagem (Bytes)	Porta
DNS	7,91Kbps	3,55 Mb	96 bytes	53
HTTP	24,75Kbps	2,59 Mb	61 bytes	80
HTTPS	12,24Kbps	126,91 Kb	265 bytes	443
ICMPV6	0bps	3,01 Kb	69 bytes	-
MDNS	0bps	301 bytes	48 bytes	5353
NTP	0bps	242 bytes	97 bytes	123
IP UNKNOWN	288bps	2,99Kb	90 bytes	-

Os resultados obtidos pelo ***Torshammer*** na Tabela 6 demonstram uma estratégia específica ao direcionar uma parte significativa de seu tráfego para o protocolo DNS, evidenciado por uma taxa instantânea de 48,15 Kbps. Assim como o *Slowloris* e o *GoldenEye*, o *Torshammer* concentra grande parte de seus recursos no ataque ao protocolo HTTP, onde o tráfego acumulado atinge 11,43 Mb, indicando uma estratégia eficaz em sobrecarregar o servidor-alvo, com uma quantidade substancial de dados transmitidos.

Ao contrário do *GoldenEye* e do *Xerxes*, o *Torshammer* mantém uma presença mais moderada no protocolo HTTPS. A taxa instantânea de 3,95 Kbps sugere uma abordagem menos intensiva, onde o tráfego acumulado atinge somente 78,77 Kb. Similarmente às duas ferramentas anteriores, o *Torshammer* também apresenta tráfego destinado a uma porta não especificada, chamada "IP UNKNOWN". A taxa instantânea de 248 bps e o tráfego acumulado de 575 bytes sugerem uma exploração de serviços não claramente identificados.

Tabela 6 - Análise instantânea das características de ataque do Torshammer

Protocolo	Taxa de tráfego instantâneo	Tráfego acumulado	Tam. da mensagem (Bytes)	Porta
DNS	48,15Kbps	1,61 Mb	93 bytes	53
HTTP	183,64Kbps	11,43 Mb	123 bytes	80
HTTPS	3,95Kbps	78,77 Kb	203 bytes	443
ICMPV6	0bps	79 bytes	56 bytes	-
MDNS	0bps	39 bytes	37 bytes	5353
NTP	0bps	176 bytes	68 bytes	123
IP UNKNOWN	248bps	575 bytes	72 bytes	-

Na análise dos ataques DoS realizada nesta pesquisa, a Tabela 7 mostra quanto tempo cada ferramenta precisou para derrubar o alvo com sucesso. A ferramenta ***Slowloris***, que tem um nível médio de tráfego, levou, em média, aproximadamente *298.0 milissegundos* para derrubar o site, considerado eficaz. O ***GoldenEye***, que também tem um nível médio de tráfego, levou em média aproximadamente *895.8 milissegundos*, que também se mostrou eficiente. O ***Xerxes***, com um nível baixo de tráfego, se destacou por derrubar o site em um tempo médio muito curto de *0.850 milissegundos*. Mesmo com menos atividade, foi notavelmente eficaz. Já o ***Torshammer***, com um nível alto de tráfego, se destacou pela persistência, atingindo um tempo médio de *8.245621 milissegundos* para derrubar o site. Pode-se notar que mesmo com um tráfego de dados baixo, o Xerxes conseguiu comprometer o alvo em um tempo muito curto. Isso destaca a eficácia única dessa ferramenta em comparação com as outras analisadas no estudo. Essa eficiência é atribuída à sua capacidade de ajustar a quantidade de tráfego de maneira inteligente, o que contribui para alcançar esse tempo curto.

Tabela 7 - Resultados dos ataques Ddos

Ferramenta	Tráfego de ataque	Nível de tráfego acumulado	Tempo médio de ataque (ms)
Slowloris	HTTP	Médio	298.0
GoldenEye	HTTP	Médio	895.8
Xerxes	HTTP	Baixo	0.850
Torshammer	HTTP	Alto	8.245621

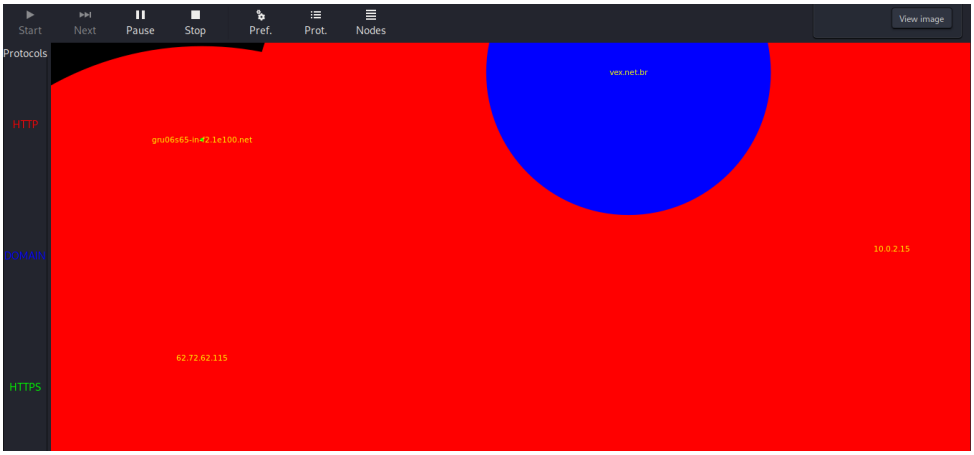
A Figura 9 oferece um instantâneo do estado inicial da rede antes do início do ataque, capturado pelo *EtherApe*.

Figura 9 - Status inicial da rede

Já nas Figuras 10, 11, 12 e 13 apresentam capturas de tela representativas do tráfego de ataque gerado pelas ferramentas *Slowloris*, *GoldenEye*, *Xerxes* e *Torshammer*, respectivamente. Estas capturas foram monitoradas pela ferramenta *EtherApe*. Na representação visual, a coloração azul destaca um volume significativo de tráfego relacionado ao protocolo DNS, enquanto a coloração vermelha indica uma atividade intensa de tráfego associada aos protocolos HTTP e a coloração verde indica o volume de tráfego relacionado ao protocolo HTTPS.

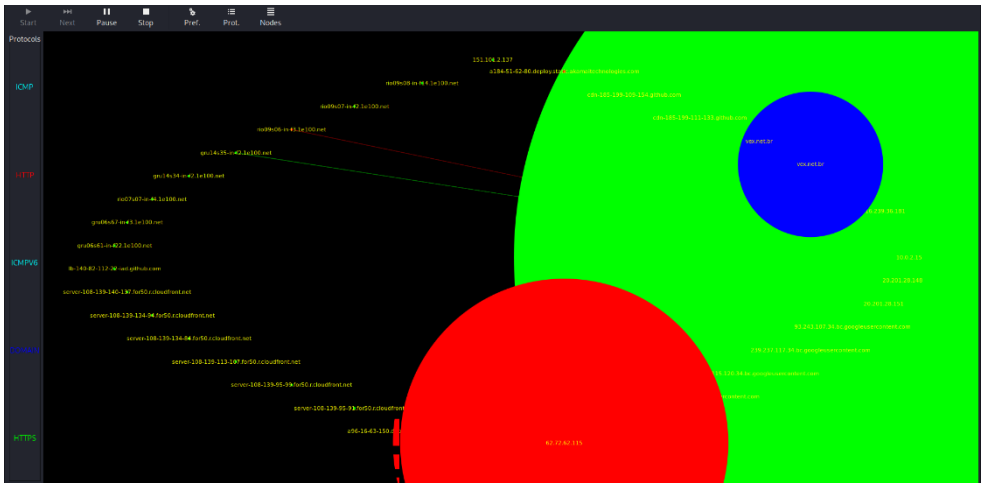
Na Figura 10, destaca-se a ênfase do *Slowloris* no protocolo HTTP, evidenciada pela carga de tráfego substancial.

Figura 10 - Status da rede após o ataque do Slowloris



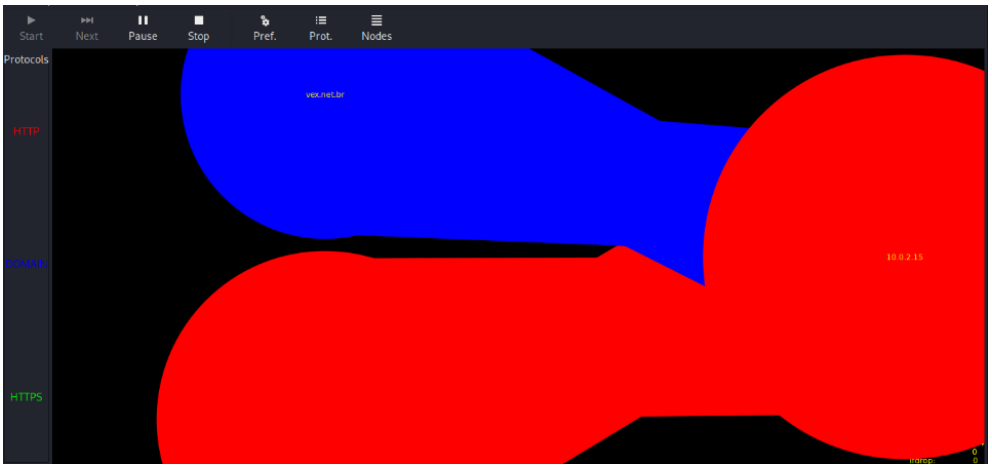
Na Figura 11, observa-se que o *GoldenEye* concentra sua atividade no protocolo HTTP, como evidenciado pela intensa carga de tráfego nesse protocolo específico. No entanto, destaca-se a diferenciação notável ao incluir uma ênfase significativa no protocolo HTTPS. A captura revela essa distinção ao mostrar uma atividade marcante em ambas as áreas, indicando a capacidade do *GoldenEye* de direcionar sua atenção para os protocolos HTTP e HTTPS durante o ataque.

Figura 11 - Status da rede após o ataque do GoldenEye



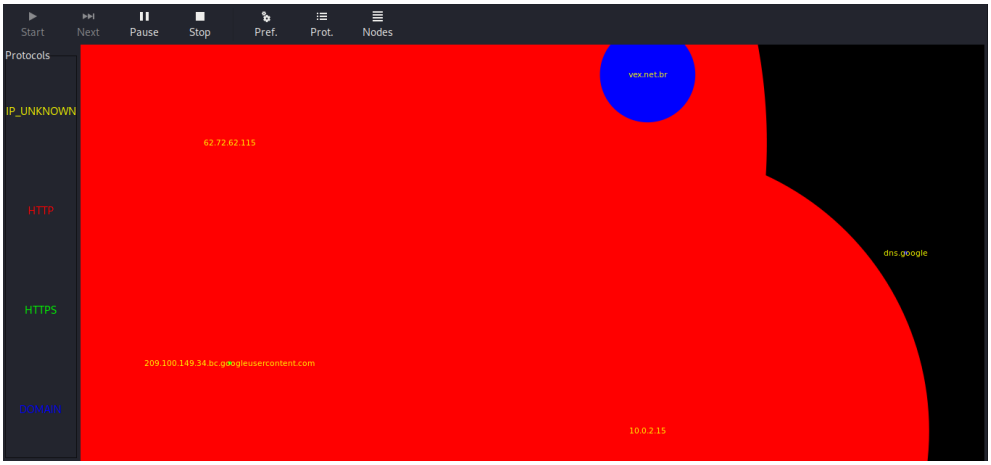
Na Figura 12, destaca-se que o *Xerxes* concentrou-se predominantemente no protocolo HTTP e DNS. A representação visual evidencia uma atenção significativa a essa camada específica, caracterizada por uma carga substancial de tráfego. A observação de uma atenção moderada ao protocolo HTTPS sugere uma abordagem semelhante às outras ferramentas.

Figura 12 - Status da rede após o ataque do Xerxes



Na Figura 13, o ataque do *Torshammer* é evidenciado pela atenção intensiva ao protocolo HTTP, representado por uma carga de tráfego significativa nessa área específica.

Figura 13 - Status da rede após o ataque do Torshammer



5 CONCLUSÃO

Neste estudo, foram analisadas quatro ferramentas destinadas a ataques distribuídos de negação de serviço *DDoS/DoS*: *Slowloris*, *GoldenEye*, *Xerxes* e *Torshammer*. Todas essas ferramentas têm em comum o foco predominante no uso do tráfego HTTP, HTTPS e DNS como método de ataque, embora apresentem abordagens distintas em suas estratégias.

O *Slowloris* se destaca por sua abordagem mais simples na execução do ataque, enquanto o *GoldenEye* e o *Xerxes* empregam lógicas mais elaboradas, com o *GoldenEye* demonstrando um volume de tráfego acumulado superior em comparação com as demais ferramentas analisadas. O *Torshammer*, ao adotar uma estratégia de pós-DoS lenta, resulta no esgotamento gradual dos recursos do alvo, exibindo um volume significativo de tráfego acumulado, semelhante ao observado no *GoldenEye*.

Os resultados obtidos no experimento indicam que o Xerxes superou significativamente o desempenho do *Slowloris*, *GoldenEye* e *Torshammer* em termos de eficiência, exigindo menos tempo para lançar com sucesso o ataque DoS/DDoS. Essa superioridade pode ser atribuída à sua abordagem mais eficaz na sobrecarga do servidor alvo. O propósito principal

desta contribuição reside na exposição das características inerentes a essas ferramentas, visando subsidiar a formulação de contramedidas eficazes contra futuros ataques DDoS.

Como trabalho futuro, sugerimos a criação de um estudo focado em mitigações específicas para cada uma dessas ferramentas, testando a eficácia dessas medidas de segurança em cenários práticos. Além disso, explorar a interação dessas ferramentas com as soluções de segurança existentes e a inclusão de testes com outras ferramentas disponíveis no mercado poderiam aprimorar ainda mais a compreensão das estratégias de defesa contra ataques Dos/DDoS. Essas abordagens futuras seriam essenciais para fortalecer as defesas cibernéticas diante da evolução constante das ameaças.

REFERÊNCIAS

BADOTRA, S.; PANDA, S. N. Snort based early ddos detection system using opendaylight and open networking operating system in software defined networking. **Cluster Computing**, Springer, v. 24, p. 501–513, 2021.

BARANI, A. M.; SINGH, J. Distributed denial of service (ddos) attacks: Taxonomy, tools, and techniques. **Journal of Network and Systems Management**, Springer, v. 29, p. 211–246, 2021.

BRASIL. **DECRETO-LEI Nº 2.848, DE 7 DE DEZEMBRO DE 1940**. 1940. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 06 Nov. 2023.

BRASIL. **LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012**. 2012. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 06 Nov. 2023.

BRASIL. **LEI Nº 12.965, DE 23 DE ABRIL DE 2014**. 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 06 Nov. 2023.

BRAVO, S.; MAURICIO, D. Ddos attack detection mechanism in the application layer using user features. In: IEEE. **2018 International Conference on Information and Computer Technologies (ICICT)**. [S.l.], 2018. p. 97–100.

BUKAC, V.; MATYAS, V. Analyzing traffic features of common standalone dos attack tools. In: SPRINGER. **Security, Privacy, and Applied Cryptography Engineering: 5th International Conference, SPACE 2015, Jaipur, India, October 3-7, 2015, Proceedings** 5. [S.l.], 2015. p. 21–40.

CARL, G. et al. Denial-of-service attack-detection techniques. **IEEE Internet Computing**, v. 10, n. 1, p. 82–89, 2006.

CHAHAL, J. K.; KAUR, P.; SHARMA, A. Distributed denial of service (ddos) attacks in software-defined networks (sdn). In: **2021 5th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)**. [S.l.: s.n.], 2021. p. 291–295.

CHOI, J. et al. A method of ddos attack detection using http packet pattern and rule engine in cloud computing environment. **Soft Computing**, Springer, v. 18, p. 1697–1703, 2014.

CLARINDO, A. B.; SILVA, K. G. G. **Relatório final detectando ataques ddos com inteligência artificia**l. Centro Universitário Sagrado Coração-UNISAGRADO, 2022.

DOULIGERIS, C.; MITROKOTSA, A. **DDoS attacks: evolution, detection, prevention, reaction, and tolerance**. [S.l.]: Springer, 2017.

DUO, W.; ZHOU, M.; ABUSORRAH, A. A survey of cyber attacks on cyber physical systems: Recent advances and challenges. **IEEE/CAA Journal of Automatica Sinica**, v. 9, n. 5, p. 784–800, 2022.

FADHLILLAH, A.; KARNA, N.; IRAWAN, A. Ids performance analysis using anomaly-based detection method for dos attack. In: **2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)**. [S.l.: s.n.], 2021. p. 18–22.

HOQUE, N.; BHATTACHARYYA, D. K.; KALITA, J. K. Botnet in ddos attacks: Trends and challenges. **IEEE Communications Surveys Tutorials**, v. 17, n. 4, p. 2242–2270, 2015.

KIM, S.-j.; KIM, B. C.; LEE, J. Y. Ddos analysis using correlation coefficient based on kolmogorov complexity. In: PARK, J. J. J. H. et al. (Ed.). **Grid and Pervasive Computing**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. p. 443–452.

KSHIRSAGAR, D.; SHAIKH, J. M. Intrusion detection using rule-based machine learning algorithms. In: **2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA)**. [S.l.: s.n.], 2019. p. 1–4.

KUMAR, S.; CARLEY, K. M. Ddos cyber-attacks network: Who's attacking whom. In: IEEE. **2016 IEEE Conference on Intelligence and Security Informatics (ISI)**. [S.l.], 2016. p. 218–218.

MACIEL, R. et al. Impact of a ddos attack on computer systems: An approach based on an attack tree model. In: IEEE. **2018 Annual IEEE International Systems Conference (SysCon)**. [S.l.], 2018. p. 1–8.

NAGPAL, B. et al. Ddos tools: Classification, analysis and comparison. In: **2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)**. [S.l.: s.n.], 2015. p. 342–346.

NAGY, B. et al. Detecting ddos attacks within milliseconds by using fpga-based hardware acceleration. In: IEEE. **NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium**. [S.l.], 2018. p. 1–4.

PATIL, R. R.; PAWALE, D. V. A survey on distributed denial-of-service (ddos) attack detection and mitigation techniques. **International Journal of Computer Science and Information Technology**, IJCSIT, v. 6, n. 1, p. 126–133, 2014.

SABRI, S.; ISMAIL, N.; HAZZIM, A. Slowloris dos attack based simulation**. IOP Conference Series: Materials Science and Engineering**, IOP Publishing, v. 1062, n. 1, p. 012029, feb 2021. Disponível em: <https://dx.doi.org/10.1088/1757-899X/1062/ 1/012029>.

SANCHEZ, O. R. et al. Feature selection evaluation towards a lightweight deep learning ddos detector. In: **ICC 2021 - IEEE International Conference on Communications**. [S.l.: s.n.], 2021. p. 1–6.

SHOREY, T. et al. Performance comparison and analysis of slowloris, goldeneye and xerxes ddos attack tools. In: **2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)**. [S.l.: s.n.], 2018. p. 318–322.

SRIHARI, V.; ANITHA, R. Ddos detection system using wavelet features and semi-supervised learning. In: MAURI, J. L. et al. (Ed.). **Security in Computing and Communications**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014. p. 291–303.

WANI, A. R. et al. Analysis and detection of ddos attacks on cloud computing environment using machine learning techniques. In: IEEE. **2019 Amity International conference on artificial intelligence (AICAI)**. [S.l.], 2019. p. 870–875.

WHITMAN, M. E.; MATTORD, H. J. **Principles of Information Security**. [S.l.]: Cengage Learning, 2016.

YIN, D.; ZHANG, L.; YANG, K. A ddos attack detection and mitigation with softwaredefined internet of things framework. **IEEE Access**, IEEE, v. 6, p. 24694–24705, 2018.

ZARGAR, S. T.; JOSHI, J.; TIPPER, D. A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. **IEEE communications surveys & tutorials**, IEEE, v. 15, n. 4, p. 2046–2069, 2013.

A. Glossário

ANOVA - Análise de Variância. DoS - Ataque de negação de serviço.
Bandwidth - Largura de banda.
CPU - Unidade central de processamento.
DDoS - Ataque de negação de serviço distribuída.
DNS - Sistema de Nomes de Domínio.
Ethernet - Tecnologia que permite a conexão física entre dispositivos como computadores, impressoras, switches e roteadores em redes locais.
FPGA - Arranjo de porta programável em campo.
FDDI - Interface de dados distribuídos de fibra.
HTTP - Protocolo de Transferência de Hipertexto.
HTTPS - Protocolo de transferência de hipertexto seguro.
ICMP - Protocolo de mensagens de controle da Internet.
ICMPv6 - Protocolo de mensagens de controle da Internet versão 6.
IGMP - Protocolo de Gerenciamento de Grupos da Internet.
IP Spoofing - É um ataque que consiste em mascarar pacotes IP utilizando endereços de remetentes falsificados.
ISDN - Rede digital de serviços integrados.

KeepAlive - Um cabeçalho que mantém uma conexão persistente entre cliente e servidor, impedindo que uma conexão interrompa intermitentemente.
MDNS - Protocolo DNS Multicast.
Modus operandi - expressão em latim que significa "modo de operação".
NTP - Protocolo para sincronização dos relógios dos computadores.
PPP - Protocolo ponto-a-ponto.
Resource - Recurso.
SDN - Rede definida por software.
SLIP - Protocolo de Internet de linha serial.
Token Ring - Protocolo de redes criado pela IBM nos anos 80.
TCP - Protocolo de Controle de Transmissão.
UDP - Protocolo de datagrama do usuário.
WLAN - Rede de área local sem fio.
XOIC - (XOR Over Internet Protocol) é uma ferramenta de ataque DDoS que se destina a sobrecarregar um servidor alvo.