CENTRO UNIVERSITÁRIO SAGRADO CORAÇÃO – UNISAGRADO

GABRIEL MONARI CANTELLI DE TOLEDO

MITIGAÇÃO DE ATAQUES DoS ATRAVÉS DO USO DO SNORT

BAURU

2024

GABRIEL MONARI CANTELLI DE TOLEDO

MITIGAÇÃO DE ATAQUES DoS ATRAVÉS DO USO DO SNORT

Trabalho de Conclusão de Curso apresentado como parte dos requisitos para obtenção do título de bacharel em Ciência da Computação - Centro Universitário Sagrado Coração.

Orientador: Prof. Dr. Elvio Gilberto da Silva
Prof. M.e Roque Maitino Neto

BAURU

2024

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD

T649m

Toledo, Gabriel Monari Cantelli de

Mitigação de ataques dos através do uso do Snort / Gabriel Monari Cantelli de Toledo. -- 2024.

18f. : il.

Orientador: Prof. Dr. Elvio Gilberto da Silva
Coorientador: Prof. M.e Roque Maitino Neto

Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Centro Universitário Sagrado Coração - UNISAGRADO - Bauru - SP

1. Detecção de intrusão. 2. Prevenção de ataques. 3. Segurança de Rede. 4. Segurança Cibernética. 5. Monitoramento de rede. I. Maitino Neto, Roque. II. Gilberto da Silva, Elvio. III. Título.

Elaborado por Lidyane Silva Lima - CRB-8/9602

GABRIEL MONARI CANTELLI DE TOLEDO

MITIGAÇÃO DE ATAQUES DoS ATRAVÉS DO USO DO SNORT

Trabalho de Conclusão de Curso apresentado como parte dos requisitos para obtenção do título de bacharel em Ciência da Computação - Centro Universitário Sagrado Coração.

Aprovado em: ___/___/____.

Banca examinadora:

_____

Prof. Dr. Robson Fernandes da Silva

Centro Universitário Sagrado Coração

_____

Prof. Dr. Patrick Pedreira Silva

Centro Universitário Sagrado Coração

_____

Titulação, Nome

Instituição

AGRADECIMENTOS

Agradeço primeiramente a Deus, pela força e pela sabedoria ao longo dessa caminhada, pela presença constante nos momentos de desafio e por me guiar até a conclusão deste trabalho.

Aos meus pais, por todo o apoio e compreensão, por sempre acreditarem em mim e me incentivarem a seguir em frente, mesmo nos momentos mais difíceis. Foram suas palavras de encorajamento e força que me sustentaram e me impulsionaram a não desistir.

Aos professores e ao coordenador do curso, que, com seus ensinamentos e orientações, foram fundamentais para o meu desenvolvimento acadêmico e profissional. Sou grato por cada conhecimento compartilhado, cada conselho dado e por todo o esforço e dedicação que empenharam em minha formação.

A todos, minha profunda gratidão por terem feito parte desta jornada e contribuído para a realização deste sonho.

"O maior inimigo do conhecimento não é a ignorância, mas a ilusão do conhecimento." (STEPHEN HAWKING)

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CPU	Central Processing Unit
DOS	Denial of Service - Ataque de negação de serviço
ICMP	Internet Control Message Protoco
IDS	Intusion Detection System
IP	Internet protocol
TCP	Transmission Control Protocol

SUMÁRIO

MITIGAÇÃO DE ATAQUES DoS ATRAVÉS DO USO DO SNORT

Gabriel Monari Cantelli de Toledo[1].Elvio Gilberto da Silva[2]. Roque Maitino Neto[2].

[1]Graduando em Ciência da Computação pelo Centro Universitário Sagrado Coração (UNISAGRADO)
bimonari@gmail.com
[2]Centro de Ciências Exatas – Centro Universitário Sagrado Coração (UNISAGRADO) -
roque.neto@unisagrado.edu.br; egsilva@unisagrado.edu.br

RESUMO

Este trabalho apresenta a detecção e prevenção de ataques em redes utilizando o Snort, uma ferramenta IDS/IPS amplamente empregada. O Snort foi configurado em uma rede virtual com três máquinas virtuais para monitorar e detectar ataques de negação de serviço (DoS) utilizando o hping3, simulando inundações TCP SYN, e ICMP direcionadas a uma máquina-alvo. Foram implementadas regras personalizadas para identificar esses padrões de tráfego malicioso, integradas ao iptables para bloqueio automático do IP de origem. A configuração do Snort como sistema de prevenção de intrusão (IPS) visou não apenas alertar sobre atividades suspeitas, mas também tomar medidas imediatas de bloqueio. Os testes em ambiente controlado demonstraram a eficácia da abordagem na mitigação dos ataques simulados. A combinação do Snort com o firewall iptables mostra-se uma solução viável para proteção de redes contra ataques DoS, contribuindo para a segurança cibernética.
Palavras-chave: detecção de intrusão, prevenção de ataques, segurança de rede, segurança cibernética, monitoramento de rede.

ABSTRACT

This work addresses the detection and prevention of network attacks using Snort, a widely used IDS/IPS tool. Initially, Snort was configured in a virtual network to monitor and detect flooding attacks such as TCP SYN Flood and ICMP Flood. Specific rules were implemented to identify these malicious patterns and then integrated with iptables for automatic blocking of attacks. Configuring Snort as an intrusion prevention system (IPS) aims not only to alert about suspicious activities but also to take immediate measures to mitigate threats. The approach's effectiveness was validated in a controlled environment, showing promising results in detecting and mitigating simulated attacks, although challenges such as false positives and the complexity of tool integration still persisted. The use of IDS/IPS systems like Snort, combined with firewall solutions, proves to be a feasible approach to protect networks against known and emerging threats, contributing to enhanced cybersecurity.
Keywords: intrusion detection, attack prevention, network security, cybersecurity, network monitoring.

1 INTRODUÇÃO

No cenário digital atual, a segurança da informação não é apenas uma prioridade, mas uma necessidade vital para organizações que dependem de serviços online confiáveis. Paralelamente, a crescente sofisticação dos ataques cibernéticos, em especial os de negação de serviço (DoS), intensifica os desafios enfrentados. Esses ataques, que buscam sobrecarregar os recursos de máquinas ou redes, podem paralisar serviços críticos em um instante, configurando uma ameaça de alta gravidade.

Este trabalho explora a configuração e utilização do Snort, uma ferramenta IDS/IPS de código aberto, em um ambiente com três máquinas virtuais, para detecção e prevenção de ataques DoS simulados usando a ferramenta hping3 no Kali Linux. Através dela, ataques de inundação TCP SYN, e ICMP foram direcionados a uma máquina Windows, representando o alvo. Simultaneamente, o Snort, operando em uma máquina intermediária, não apenas identificou padrões maliciosos no tráfego, mas também desencadeou o bloqueio automático do IP atacante via firewall iptables.

O aumento dos serviços online e das ameaças cibernéticas trazem também aumento da preocupação da população e de empresas em todo o mundo em relação a sua segurança. Este trabalho foi realizado buscando mostrar o funcionamento dessas ferramentas e contribuir com o desenvolvimento de estratégias de defesa eficazes contra os ataques DoS, sendo assim trazendo mais segurança contra as ameaças cibernéticas que estão cada vez mais comuns no dia de hoje.

2 REVISÃO DE LITERATURA

2.1 DETECÇÃO DE INTRUSÕES

A detecção de intrusões é fundamental para identificar atividades maliciosas ou anômalas em redes. Sistemas de Detecção de Intrusões (IDS) são classificados em baseados em assinaturas e anomalias. IDS baseados em assinaturas detectam ataques conhecidos, enquanto os baseados em anomalias identificam comportamentos anômalos, possivelmente detectando novos ataques, mas com maior chance de falsos positivos (Liao *et al*., 2013).

2.2 ATAQUES DOS

Um ataque de negação de serviço (Denial of Service, DoS) é uma tentativa maliciosa de tornar um recurso de rede indisponível para seus usuários legítimos, sobrecarregando-o com uma quantidade massiva de solicitações, de forma que o sistema alvo não consiga processar as requisições ou se torne extremamente lento. A principal intenção dos ataques DoS é interromper o funcionamento normal de serviços, aplicativos ou redes, resultando em perdas significativas tanto para os usuários quanto para as empresas (Stallings, 2018). Existem diferentes formas de ataques DoS, incluindo ataques de esgotamento de recursos e de exploração de vulnerabilidades. No primeiro caso, o atacante tenta sobrecarregar os recursos de hardware ou software do sistema alvo, como largura de banda, memória ou poder de processamento (Zhang et al., 2016). Um exemplo disso é o ataque "SYN flood", no qual o invasor envia uma quantidade enorme de pacotes de solicitação de conexão (SYN) sem nunca concluir o handshake TCP, esgotando a capacidade do servidor para aceitar novas conexões (Cisco, 2020).

2.3 SNORT

O Snort é uma ferramenta amplamente utilizada para a detecção de intrusões em redes, criada por Martin Roesch em 1998. O Snort é compatível com diversos sistemas operacionais, incluindo o Windows, Linux e Mac OS, porém sua maior eficiência pode ser

obtida no Linux. Ele funciona como um Sistema de Detecção de Intrusões (IDS), analisando o tráfego de rede em tempo real para identificar atividades suspeitas ou maliciosas, baseando-se em um conjunto de regras pré-definidas. Devido à sua flexibilidade para monitoramento em redes tanto IPv4 como IPv6, o Snort é utilizado tanto em ambientes empresariais quanto em redes domésticas, tornando-se uma das soluções mais populares para segurança de rede (Roesch, 1999). O Snort opera principalmente como um IDS baseado em assinatura, o que significa que ele detecta intrusões ao comparar o tráfego de rede com assinaturas conhecidas de atividades maliciosas. Esse mecanismo possibilita a detecção de uma ampla gama de ameaças, como varreduras de porta, ataques de negação de serviço e tentativas de exploração de vulnerabilidades conhecidas (Sommer & Paxson, 2010). Além disso, o Snort também oferece funcionalidades de monitoramento de pacotes e prevenção de intrusões (IDS/IPS), podendo atuar de maneira proativa para bloquear tentativas de ataque (Caswell & Beale, 2004). A flexibilidade e a capacidade de adaptação são características chave do Snort. Ele permite a criação de regras personalizadas, permitindo aos administradores de rede adequar as configurações do IDS às necessidades específicas do ambiente protegido. Adicionalmente, a comunidade ativa ao redor do Snort contribui significativamente para a manutenção e evolução da ferramenta, desenvolvendo novas assinaturas e funcionalidades para enfrentar as ameaças emergentes (Patel et al., 2013).

2.4 IPTABLES

O iptables é uma ferramenta de firewall utilizada em sistemas Linux para controle de tráfego de rede com pacotes IPv4. Ele permite criar regras que filtram, bloqueiam ou encaminham pacotes com base em critérios como endereço IP, porta e protocolo. Amplamente usado para proteção de redes, o iptables é eficaz na defesa contra ataques e na gestão de acesso, sendo uma solução flexível e robusta para segurança de sistemas (Müller, 2017).

3 OBJETIVO

Investigar os ataques de negação de serviço (DoS), utilizando o hping3 no ambiente Kali Linux, e propor uma estratégia de defesa eficaz utilizando o Snort como sistema de detecção de intrusões (IPS).

4 METODOLOGIA

O estudo propôs a análise de um teste para detecção de intrusões em uma rede realizando ataques de negação de serviço (DoS) e depois propondo uma estratégia de bloqueio através do uso do Snort. Seguindo as etapas descritas abaixo:

A tabela a seguir mostra as vantagens e desvantagens da escolha do Snort como ferramenta de detecção IDS em relação a ferramentas similares, sendo a maior motivação a facilidade de uso e de configurações em relação a outras ferramentas.

Tabela 1 - Comapração

	Vantagens	**Desvantagens**

Snort	• Ampla adoção e comunidade ativa, oferecendo suporte e atualizações contínuas. • Facilidade de uso com regras predefinidas e ampla documentação. • Integração com ferramentas de gerenciamento como Snorby, BASE e Sguil.	• Desempenho limitado devido ao processamento single-threaded, o que pode ser insuficiente em ambientes com tráfego intenso.
Suricata	• Suporte nativo a multi-threading, permitindo alto desempenho em ambientes com múltiplos núcleos. • Funcionalidades avançadas, como inspeção de protocolos da camada de aplicação e capacidade nativa de atuar como IPS.	• Curva de aprendizado mais íngreme, tornando a configuração inicial mais complexa.
Zeek	• Foco em análise profunda de tráfego, ideal para investigação forense e detecção de anomalias. • Extensibilidade por meio de scripts personalizados, oferecendo grande flexibilidade.	• Complexidade elevada, demandando conhecimento avançado para configuração e uso. • Não é otimizado para detecção baseada em assinaturas.

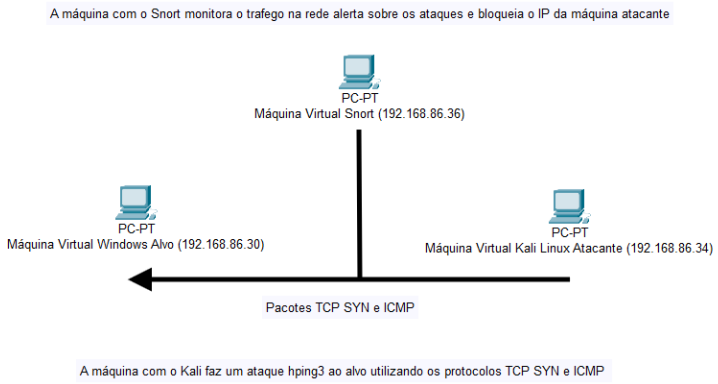
Fonte: Elaborada pelo autor

4.1 SELEÇÃO E CONFIGURAÇÃO DO AMBIENTE DE TESTES

a) Foi configurado um ambiente de teste com três máquinas virtuais no VirtualBox: uma com o Kali Linux para lançar os ataques (atacante), uma Windows (alvo) e uma dedicada ao Snort para monitorar e defender a rede.

b) A topologia configurada da Figura 1 foi uma rede em que a máquina com o Snort monitorava o tráfego e estava configurada para bloquear automaticamente o IP da máquina atacante ao identificar um ataque.

Figura 1 - Topologia do modelo de funcionamento do Ataque/Defesa



Fonte: Elaborada pelo autor

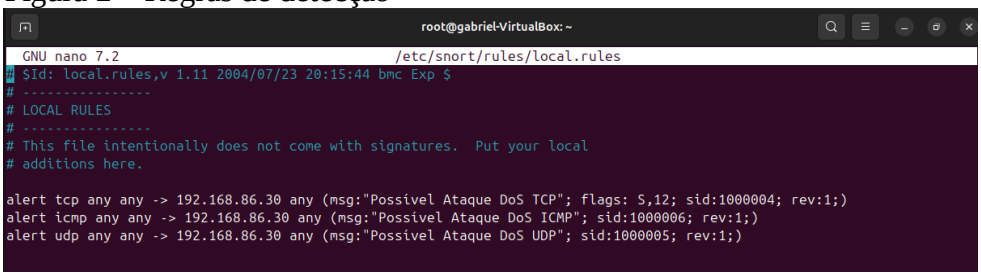
4.2 REALIZAÇÃO DE ATAQUES DOS COM HPING3

a) Foram realizados ataques de inundação TCP SYN, e ICMP, utilizando a ferramenta hping3 no Kali Linux, direcionados à máquina Windows (alvo).
b) Cada ataque foi monitorado para avaliar a sobrecarga no sistema alvo e entender como o tráfego malicioso afetava a rede.

4.3 IMPLEMENTAÇÃO E CONFIGURAÇÃO DO SNORT

Em um ambiente de testes realizados na máquina virtual foram configuradas um conjunto de regras customizadas para detectar o tráfego malicioso como mostra a figura 2.

Figura 2 – Regras de detecção



Fonte: Elaborada pelo autor

Cada regra tem as seguintes funções:

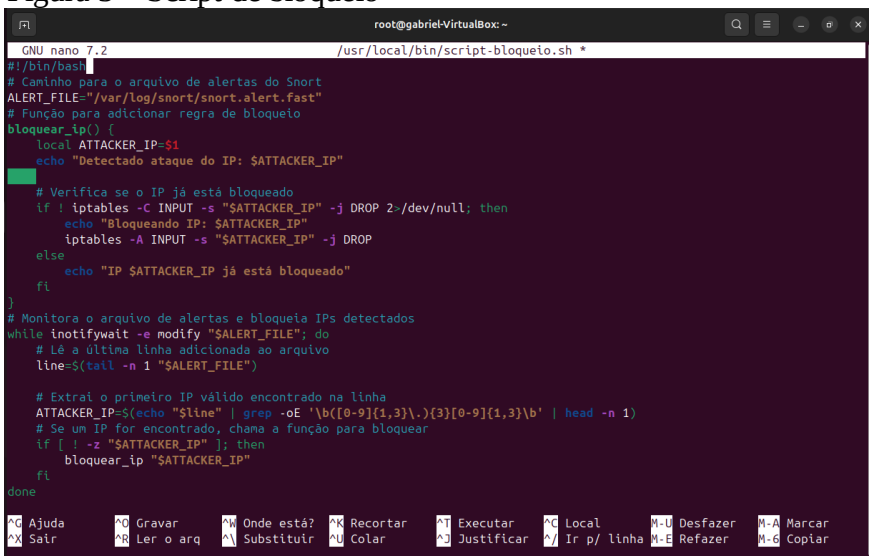
a) Monitoram pacotes TCP e ICMP que tenham como destino o IP da máquina alvo (192.168.86.23).
b) Gerar Alertas: Quando um padrão de tráfego condizente com a regra é identificado, o Snort emite um alerta no console e registra a atividade nos logs.

4.4 SCRIPT DE BLOQUEIO

Além disso, como é mostrado na figura 3, foi utilizado um script para automatizar o bloqueio do IP da máquina atacante, baseado nos alertas gerados pelo Snort.

Para impedir que a máquina atacante continuasse enviando pacotes após a detecção do ataque, foi implementado um mecanismo de bloqueio automático. Este mecanismo utilizou um script que monitorava os logs do Snort em tempo real, identificava os IPs suspeitos e adicionava regras ao firewall (iptables) para bloquear todo o tráfego proveniente do IP identificado.

Figura 3 – Script de bloqueio



Fonte: Elaborada pelo autor

O script monitorava o arquivo /var/log/snort/alert, onde o Snort registrava os alertas, o arquivo /tmp/blocked_ips.txt armazena os IPs que já foram bloqueados para evitar redundâncias. E por último a ferramenta iptables foi utilizada para adicionar regras ao firewall, impedindo que o IP atacante continuasse enviando pacotes à máquina alvo.

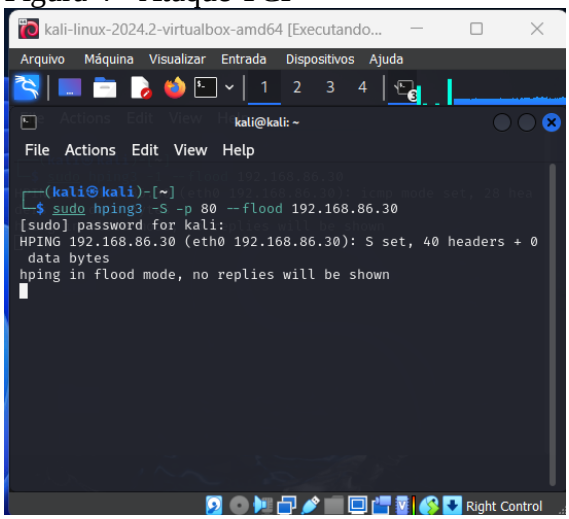
5 RESULTADOS E DISCUSSÃO

A realização dos experimentos nos permitiu observar os impactos dos ataques (DoS) e averiguar a eficiência do Snort como um sistema de detecção e bloqueio dos ataques. Analisando os resultados obtidos, pode-se dividir em três partes principais: impacto dos ataques na máquina alvo, desempenho do Snort na detecção e bloqueio, e limitações.

5.1 ATAQUES

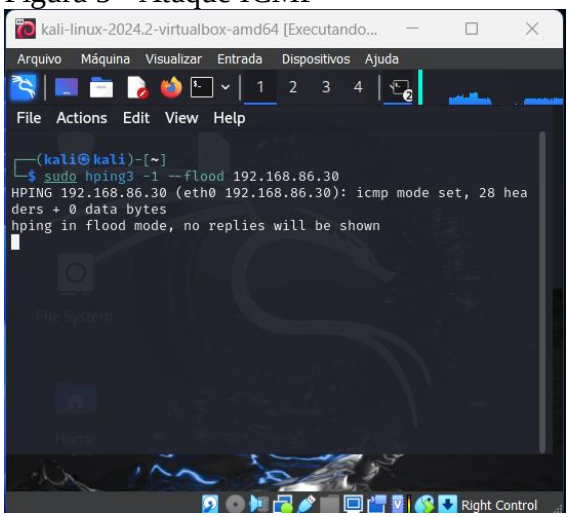
A figura 4 mostra a realização de um ataque hping3 do tipo TCP pela máquina atacante direcionado a máquina alvo de IP 192.168.86.30, enquanto a figura 5 mostra um ataque lançado simultaneamente do tipo ICMP direcionado ao alvo buscando sobrecarregar os recursos de processamento da máquina alvo.

Figura 4 - Ataque TCP



Fonte: Elaborada pelo autor

Figura 5 - Ataque ICMP



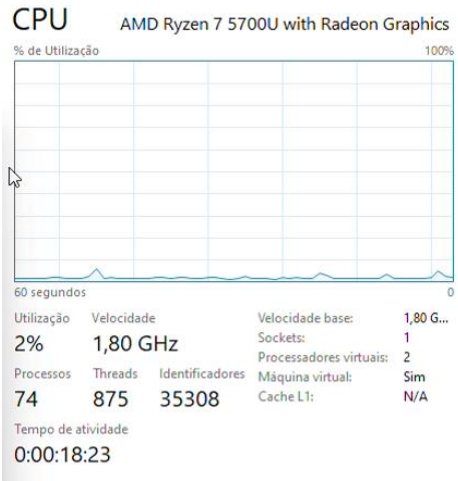
Fonte: Elaborada pelo autor

5.2 IMPACTO DOS ATAQUES

Durante os ataques DoS realizados pela máquina com Kali Linux utilizando a ferramenta hping3, observou-se uma sobrecarga significativa na máquina alvo. O ataque sobrecarregou os recursos do alvo, comprometendo sua capacidade de resposta. Os principais indicadores de impacto foram:

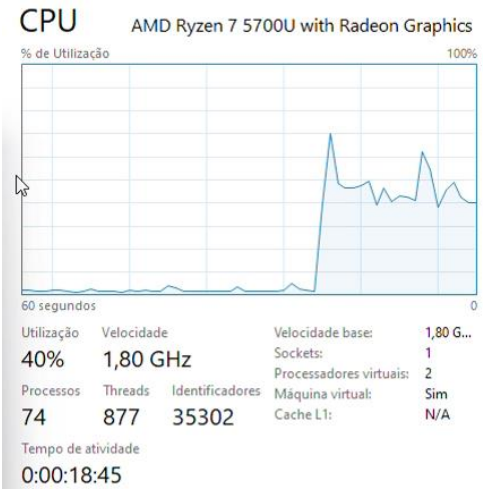
a) Consumo Elevado da CPU: Durante o ataque, é mostrado pelas figuras 6 e 7 como consumo de CPU na máquina alvo aumentou drasticamente, o que indica uma exaustão de recursos pelo volume de pacotes processados. Esse efeito pode ser ilustrado com gráficos que mostram o uso de CPU e memória antes, durante e após o ataque.

Figura 6 – Uso da CPU antes do ataque



Fonte: Elaborada pelo autor

Figura 7 – Uso da CPU durante o ataque



Fonte: Elaborada pelo autor

b) Atrasos na Resposta e Comprometimento Geral: O tempo de resposta da máquina aumentou, tornando-a lenta e, eventualmente, inacessível para outras operações de rede. Esses resultados demonstram como um ataque DoS pode impactar máquinas não protegidas.

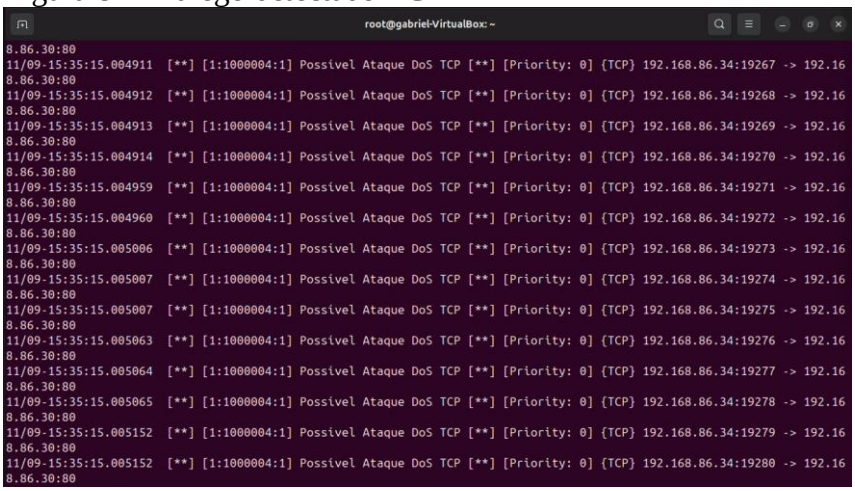
Esses resultados mostraram a vulnerabilidade de sistemas sem proteção e a necessidade de medidas de defesa contra os ataques DoS.

5.3 DESEMPENHO DO SNORT NA DETECÇÃO E BLOQUEIO DOS ATAQUES

Depois de configurar o Snort com regras específicas para detectar o tráfego anômalo dos ataques DoS, os testes mostraram nas figuras 8 e 9 que o Snort conseguiu identificar e bloquear o ataque com exelencia como mostram as figuras 10, 11 e 12. Os resultados principais incluem:

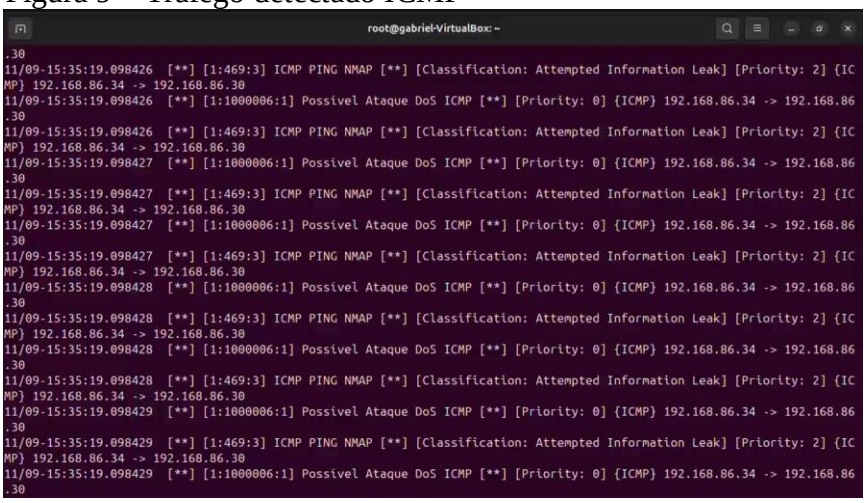
a) Detecção Rápida dos Ataques: O Snort detectou o tráfego malicioso logo após o início do teste. Os alertas gerados no console de monitoramento mostraram a origem do ataque, o tipo de protocolo utilizado e o IP de origem da ameaça detectada.

Figura 8 – Tráfego detectado TCP



Fonte: Elaborada pelo autor

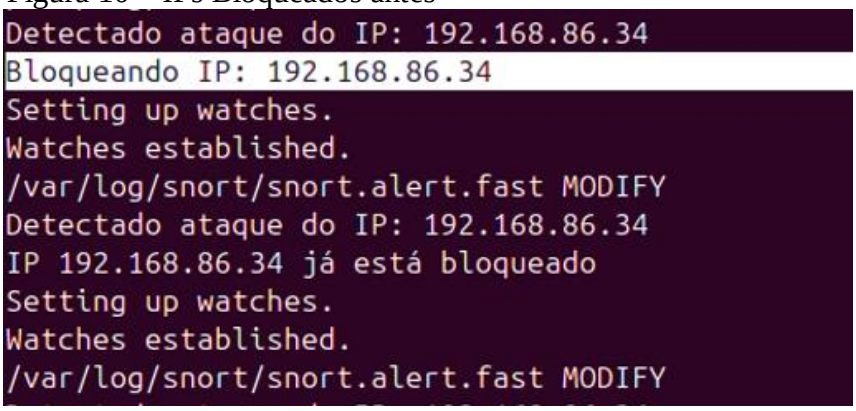
Figura 9 – Tráfego detectado ICMP



Fonte: Elaborada pelo autor

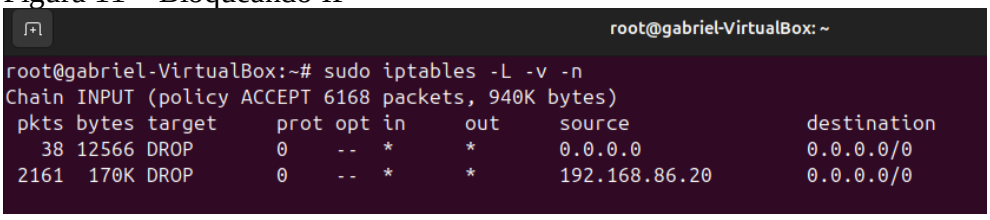
b) Bloqueio do IP Atacante: Depois de detectar o ataque, o Snort bloqueou automaticamente o IP da máquina atacante, impedindo que ela continuasse enviando pacotes à máquina alvo. Reestabelecendo os recursos do alvo.

Figura 10 – IPs Bloqueados antes



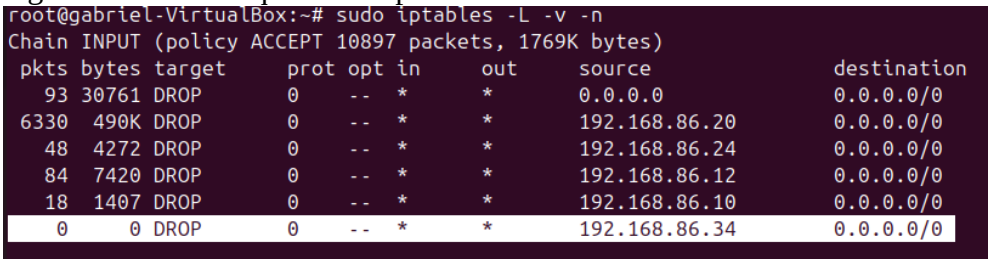
Fonte: Elaborada pelo autor

Figura 11 – Bloqueando IP



Fonte: Elaborada pelo autor

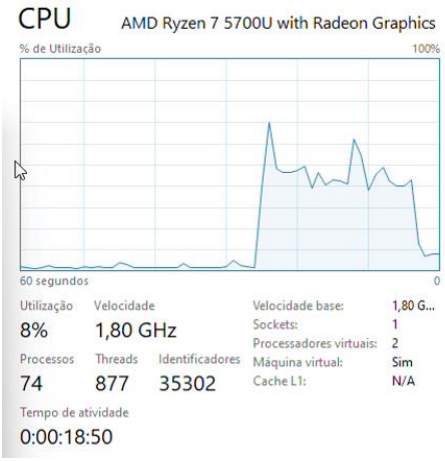
Figura 12 – IPs Bloqueados depois



Fonte: Elaborada pelo autor

c) Redução do Impacto após o Bloqueio: Uma vez que o IP da máquina atacante foi bloqueado, a figura 13 mostra como o consumo de recursos na máquina alvo foi significativamente reduzido. A conectividade foi gradualmente restabelecida, mostrando a eficácia da resposta do Snort.

Figura 13 – CPU após Bloqueio do IP da máquina atacante



Fonte: Elaborada pelo autor

5.4 LIMITAÇÕES E ANÁLISE DE RESULTADOS

Este estudo investigou os impactos dos ataques DoS em uma máquina alvo e avaliou a eficácia do Snort como um sistema de detecção e resposta para mitigar esses ataques. Apesar do Snort ter se mostrado eficaz, algumas limitações foram encontradas:

a) Limitação para ataques com Spoofing: Não é possível fazer o bloqueio de ataques com spoofing, pois o snort detecta apenas os IPs falsos e não o verdadeiro IP atacante, mas isso pode ser solucionado utilizando outras ferramentas como o Suricata e o Wireshark complementando o Snort para analisar mais detalhadamente os pacotes.
b) Ambiente de testes controlado: Os experimentos foram realizados em máquinas virtuais com tráfego simulado, então os resultados podem ser diferentes em redes reais com maior complexidade e volume de tráfego.
c) A ferramenta Iptables é limitada a IPs apenas do tipo IPv4, Assim não sendo eficiente no uso de redes com IPv6, porém isso pode ser ajustado utilizando uma ferramenta chamada Ip6tables, alcançando um nível maior de segurança.

Esses pontos mostram a importância de configurar o Snort corretamente e de realizar ajustes periodicos em ambientes reais.

6 CONSIDERAÇÕES FINAIS

Após a finalização da simulação conclui-se que a estratégia para mitigar os ataques funcionou corretamente atingindo os objetivos do estudo e destacando os tópicos abaixo:

a) Ataques DoS podem comprometer severamente máquinas não protegidas, causando exaustão de recursos, queda na conectividade e comprometimento das operações.

b) O Snort demonstrou eficácia como ferramenta de defesa, identificando e bloqueando o tráfego malicioso com rapidez e mitigando os impactos do ataque.
c) A necessidade de configurações especificas mostra que devemos sempre realizar manutenções periódicas nas configurações do snort, para ter sua eficiência garantida contra novas e diferentes tipos de ameaças e cenários.

Apesar dos testes terem sido realizados em um ambiente controlado, os resultados mostram que o Snort pode ser uma solução eficaz para proteção de dispositivos contra ataques DoS.

REFERÊNCIAS

CASWELL, B.; BEALE, J. *Snort Intrusion Detection and Prevention Toolkit*. Rockland: Syngress, 2004.

CISCO. **What is a DoS attack?** 2020. Disponível em: https://www.cisco.com. Acesso em: 24 nov. 2024.

HAWKING, S. O maior inimigo do conhecimento não é a ignorância, mas a ilusão do conhecimento. Frase atribuída.

LIAO, H. J. et al. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, v. 36, n. 1, p. 16–24, 2013.

MÜLLER, M. Linux iptables Pocket Reference. 1. ed. Sebastopol: O'Reilly Media, 2017. 102 p.

PATEL, H.; MODI, C.; JOSHI, A. Recent advances in intrusion detection systems. *International Journal of Computer Applications*, v. 68, n. 25, p. 34–42, 2013.

ROESCH, M. Snort: Lightweight intrusion detection for networks. *Proceedings of the 13th USENIX Conference on System Administration*, p. 229–238, 1999.

SOMMER, R.; PAXSON, V. Outside the closed world: On using machine learning for network intrusion detection. *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, p. 305–316, 2010.

STALLINGS, W. *Criptografia e segurança de redes: princípios e práticas*. 6. ed. São Paulo: Pearson, 2018.

ZHANG, H.; XU, J.; ZHANG, H. Detecting and defending against SYN flooding attacks. *Computers & Security*, v. 62, p. 80–92, 2016.