



**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO
TOCANTINS
CAMPUS ARAGUATINS
CURSO SUPERIOR DE LICENCIATURA EM COMPUTAÇÃO**

MARCELO GOMES DA SILVA

**DETECÇÃO DE ATAQUES SMURF: UM MODELO BASEADO EM ANÁLISE DE
PACOTES ICMP**

**ARAGUATINS - TO
2024**

MARCELO GOMES DA SILVA

**DETECÇÃO DE ATAQUES SMURF: UM MODELO BASEADO EM ANÁLISE DE
PACOTES ICMP**

Trabalho de Conclusão de Curso apresentado à
Coordenação do Curso Licenciatura em
Computação da Unidade *Araguatins*, do Instituto
Federal do Tocantins, como exigência à obtenção
do título de Licenciado em Computação.

Orientador(a): Me. Adeilson Marques da Silva
Cardoso

ARAGUATINS - TO
2024

Dados Internacionais de Catalogação na Publicação (CIP)
Bibliotecas do Instituto Federal do Tocantins

S586d Silva, Marcelo Gomes da
Detecção de ataques smurf : um modelo baseado em análise de
pacotes ICMP / Marcelo Gomes da Silva. – ARAGUATINS, TO, 2024.
26 p. : il. color.

Trabalho de Conclusão de Curso (Licenciatura em Computação)
– Instituto Federal de Educação, Ciência e Tecnologia do Tocantins,
Campus Araguatins, ARAGUATINS, TO, 2024.

Orientador: Me. Adeilson Marques da Silva Cardoso

1. Segurança cibernética. 2. Negação de Serviço. 3. Ataque
Smurf. I. Cardoso, Adeilson Marques da Silva. II. Título.

CDD 004

A reprodução total ou parcial, de qualquer forma ou por qualquer meio, deste documento é autorizada para fins
de estudo e pesquisa, desde que citada a fonte.

**Elaborado pelo sistema de geração automática de ficha catalográfica do IFTO com os dados fornecidos
pelo(a) autor(a).**

FOLHA DE APROVAÇÃO

12/18/24, 11:13 AM

SEI/IFTO - 2599876 - Documento padrão



Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Tocantins
Campus Araguatins

FOLHA DE APROVAÇÃO

TÍTULO: DETECÇÃO DE ATAQUES SMURF: UM MODELO BASEADO EM ANÁLISE DE PACOTES ICMP

AUTORA: MARCELO GOMES DA SILVA

ORIENTADOR: PROF. ME. ADEILSON MARQUES DA SILVA CARDOSO

Trabalho de Conclusão de Curso apresentado ao Instituto Federal de Educação, Ciência e Tecnologia do Tocantins, *Campus Araguatins*, como parte das exigências para a conclusão do Curso de Licenciatura em Computação.

Aprovado em 12 de dezembro de 2024.

PROF. ME. ADEILSON MARQUES DA SILVA CARDOSO
Presidente da Banca

PROF. ESP. ANCELMO FRANK COELHO CASTRO
Primeiro avaliador

PROF. ESP. JUDSON FRANCIEL BARROS SILVA
Segundo avaliador



Documento assinado eletronicamente por **Ancelmo Frank Coelho Castro, Coordenador**, em 12/12/2024, às 18:17, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Adeilson Marques da Silva Cardoso, Servidor**, em 12/12/2024, às 18:17, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Judson Franciel Barros Silva, Servidor**, em 12/12/2024, às 18:19, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site http://sei.iftoc.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2599876** e o código CRC **37D1695E**.

Referência: Processo nº 23233.024588/2024-34

SEI nº 2599876

AGRADECIMENTOS

Agradeço primeiramente a Deus, por nos guiar pelos caminhos corretos, e por permitir alcançar os objetivos em todo o percurso traçado. Agradecer a minha família que sempre me apoiou e pelos incentivos a concluir o curso, principalmente pela Minha Esposa Sayonara dos Santos Cardoso, meus filhos, Sabrina Cardoso Lima e Matteo Cardoso da Silva, por estarem me incentivando diretamente ou indiretamente, e por meu orientador, que mesmo diante de todas as situações, continuou me apoiando e não deixou desistir. Certamente ao longo da trajetória, pode desfrutar dos aprendizados e das amizades construídas ao longo do tempo. E principalmente a família IFTO – Campus Araguatins, por prover momentos únicos na formação do ensino.

RESUMO

A segurança cibernética protege sistemas e redes, garantindo disponibilidade, integridade e confidencialidade. Com o aumento da conectividade global, ataques cibernéticos, como os de negação de serviço (DoS), tornam-se mais frequentes e perigosos, sobrecarregando sistemas com tráfego malicioso. O ataque Smurf, identificado nos anos 1990, exemplifica um tipo de DoS que utiliza o Protocolo ICMP para inundar alvos. Ele envia pacotes ICMP Echo Request para endereços de broadcast, falsificando o endereço de origem, o que faz os dispositivos da rede responderem simultaneamente ao alvo, causando sobrecarga e interrupção dos serviços. Mesmo com sua origem antiga, o ataque Smurf ainda ameaça redes vulneráveis e dispositivos IoT, que ampliam as possibilidades de ataque. Abordagens tradicionais para detecção enfrentam dificuldades, como alta incidência de falsos positivos e dependência de configurações específicas, destacando a necessidade de soluções mais eficazes. Este estudo propõe desenvolver um modelo para detectar ataques Smurf, analisando padrões de tráfego ICMP, criando algoritmos específicos e avaliando sua eficácia em testes simulados. A pesquisa busca fortalecer a segurança de redes digitais, protegendo infraestruturas críticas contra ameaças modernas e proporcionando uma solução adaptável a diferentes ambientes.

Palavras-chave: Segurança cibernética, Negação de Serviço, Ataque Smurf.

RESUMO EM LÍNGUA ESTRANGEIRA

Cybersecurity protects systems and networks, ensuring availability, integrity and confidentiality. With increasing global connectivity, cyber attacks, such as denial of service (DoS), become more frequent and dangerous, overwhelming systems with malicious traffic. The Smurf attack, identified in the 1990, exemplifies a type of DoS that uses the ICMP Protocol to flood targets. It sends ICMP Echo Request packets to broadcast addresses, spoofing the source address, which causes network devices to respond simultaneously to the target, causing overload and interruption of services. Even with its ancient origins, the Smurf attack still threatens vulnerable networks and IoT devices, which expands the possibilities of attack. Traditional approaches to detection face difficulties such as high incidence of false positives and dependence on specific configurations, highlighting the need for more effective solutions. This study proposes to develop a model to detect Smurf attacks, analyzing ICMP traffic patterns, creating specific algorithms and evaluating their effectiveness in simulated tests. The research seeks to strengthen the security of digital networks, protecting critical infrastructures against modern threats and providing a solution adaptable to different environments.

Keywords: Cybersecurity, Denial of Service, Smurf Attack.

LISTA DE SIGLAS

CPU	Unidade Central De Processamento
DDos	Ataque De Negação De Serviço Distribuído
Dos	Negação De Serviço
ICMP	Protocolo De Mensagens De Controle De Internet
IoT	Internet Das Coisas
TFP	Taxa De Falso Positivo
TVP	Taxa De Verdadeiro Positivo

SUMÁRIO

1 INTRODUÇÃO	11
1.1 Objetivos	12
<i>1.1.1 Objetivo Geral</i>	12
<i>1.1.2 Objetivos Específicos</i>	12
2. REVISÃO DA LITERATURA	14
2.1 Evolução dos Ataques de Negação de Serviço	14
2.2 O Ataque Smurf	14
2.3 Detecção e Mitigação de Ataques Smurf	15
2.4 Lacunas na Literatura e Justificativa da Pesquisa	16
3. MATERIAL E MÉTODOS	17
3.1 Cenário Experimental	17
<i>3.1.1 Configuração das Máquinas Virtuais</i>	17
3.2 Ferramentas Utilizadas	17
<i>3.2.1 Linguagem de Programação e Bibliotecas</i>	17
<i>3.2.2 Ferramentas de Teste</i>	18
3.3 Configuração dos Testes Simulados	18
3.4 Algoritmo de Detecção	18
<i>3.4.1 Descrição das Principais Funcionalidades</i>	20
3.5 Critérios de Avaliação	20
4. RESULTADOS E DISCUSSÃO	22
4.1 Resultados Obtidos nos Cenários Simulados	22
<i>4.1.1 Taxas de Detecção</i>	22
<i>4.1.2 Tempo de Resposta</i>	22
4.2 DISCUSSÃO DAS LIMITAÇÕES	23
5. CONSIDERAÇÕES FINAIS	25
REFERÊNCIAS	26

1 INTRODUÇÃO

A segurança cibernética tornou-se um pilar essencial no mundo digital, garantindo a disponibilidade, a integridade e a confidencialidade de sistemas e redes. Com o aumento exponencial da conectividade global, ataques cibernéticos têm se tornado mais frequentes e sofisticados, ameaçando a estabilidade de infraestruturas críticas e gerando impactos financeiros e operacionais significativos.

Entre os ataques mais prejudiciais estão os ataques de negação de serviço (DoS), projetados para comprometer a disponibilidade de sistemas ao sobrecarregá-los com tráfego malicioso. Um exemplo notável dessa categoria é o ataque Smurf, que explora vulnerabilidades em redes mal configuradas, tornando-se uma ameaça persistente, mesmo décadas após sua identificação.

O ataque Smurf, identificado inicialmente na década de 1990, exemplifica uma forma específica de ataque DoS que explora o Protocolo de Mensagens de Controle da Internet (ICMP) para inundar um sistema-alvo com tráfego malicioso. Esse ataque opera enviando pacotes ICMP Echo Request para endereços de broadcast com o endereço de origem falsificado, fazendo com que múltiplos dispositivos na rede respondam simultaneamente ao sistema vítima, resultando em uma sobrecarga que pode levar à degradação ou interrupção completa dos serviços (WIKIPEDIA, 2024).

Apesar de sua origem histórica, o ataque Smurf permanece relevante no cenário atual de cibersegurança. Estudos indicam que redes mal configuradas continuam vulneráveis a ataques de amplificação baseados em ICMP, evidenciando a necessidade contínua de vigilância e atualização de práticas de segurança. Além disso, a evolução das técnicas de ataque e a crescente complexidade das redes modernas, impulsionadas pela proliferação de dispositivos da Internet das Coisas (IoT), ampliam a superfície de ataque, tornando imperativo o desenvolvimento de métodos de detecção e mitigação mais eficazes.

O ataque Smurf opera enviando pacotes ICMP Echo Request para endereços de broadcast de uma rede, utilizando um endereço de origem falsificado (spoofing). Isso faz com que todos os dispositivos na rede respondam ao IP falsificado, resultando em uma amplificação massiva de tráfego direcionada ao sistema vítima.

O impacto é a sobrecarga do sistema alvo, que se torna incapaz de processar solicitações legítimas, levando à interrupção parcial ou completa dos serviços. A simplicidade do ataque e sua eficácia em redes desprotegidas ou mal configuradas mantêm sua relevância no panorama atual da segurança cibernética.

Embora existam diversas abordagens para a detecção de ataques de negação de serviço, muitas delas apresentam limitações, como dependência de configurações específicas de rede ou alta incidência de falsos positivos. Isso evidencia a necessidade de métodos mais eficazes, que combinem precisão na identificação de tráfego malicioso com baixa interferência em operações legítimas. Dada a importância crescente de redes complexas e heterogêneas, como aquelas envolvendo dispositivos IoT, um modelo específico para detectar ataques Smurf pode preencher uma lacuna crítica na segurança de redes.

Este estudo tem como objetivo geral desenvolver e validar um modelo eficaz para a detecção de ataques Smurf em redes digitais, utilizando a análise de pacotes ICMP. Para isso, os objetivos específicos incluem: (i) analisar padrões de tráfego associados ao ataque Smurf, (ii) desenvolver um algoritmo de detecção baseado na análise de pacotes ICMP, (iii) simular cenários de ataque em ambientes controlados e (iv) avaliar o desempenho do modelo, considerando taxas de detecção e tempo de resposta. Com isso, espera-se contribuir para a proteção de redes contra ataques de negação de serviço, fortalecendo práticas de segurança cibernética e oferecendo uma solução adaptável a diferentes configurações de rede.

1.1 Objetivos

1.1.1 Objetivo Geral

Desenvolver e avaliar um modelo de detecção para ataques Smurf, capaz de identificar padrões de tráfego malicioso, reduzindo falsos positivos e garantindo adaptabilidade a diferentes configurações de rede.

1.1.2 Objetivos Específicos

1. Analisar os padrões de tráfego associados ao ataque Smurf:

- Estudar as características específicas dos pacotes ICMP Echo Request

e Echo Reply envolvidos no ataque, identificando os parâmetros que diferenciam tráfego malicioso de legítimo.

2. Desenvolver um algoritmo de detecção com base na análise de pacotes

ICMP:

- Implementar um modelo utilizando bibliotecas como Scapy para monitoramento de pacotes em tempo real, detectando padrões associados a ataques Smurf.

3. Simular cenários de ataques Smurf em ambientes controlados:

- Utilizar máquinas virtuais configuradas como atacantes e vítimas para testar o modelo, garantindo a reprodutibilidade e a confiabilidade dos resultados.

4. Avaliar o desempenho do modelo de detecção:

- Medir taxas de verdadeiro positivo, falso positivo, precisão e tempo de resposta em diferentes configurações de rede para verificar a eficácia do modelo.

2. REVISÃO DA LITERATURA

A segurança cibernética tem evoluído significativamente, especialmente no contexto dos ataques de negação de serviço (DoS) e suas variantes distribuídas (DDoS). Dentre esses, o ataque Smurf destaca-se por explorar vulnerabilidades no protocolo ICMP, causando sobrecarga em sistemas alvos. Esta revisão aborda a evolução dos ataques DoS, com ênfase no ataque Smurf, e discute metodologias recentes de detecção e mitigação, destacando suas limitações e as lacunas que a presente pesquisa busca preencher.

2.1 Evolução dos Ataques de Negação de Serviço

Os ataques DoS têm como objetivo tornar sistemas ou redes indisponíveis para usuários legítimos, geralmente sobrecarregando os recursos do alvo. Com o tempo, esses ataques evoluíram de simples tentativas de esgotamento de recursos para estratégias mais complexas, como os ataques DDoS, que utilizam múltiplas fontes para amplificar o impacto (YANNIS, 2024). O ataque Smurf, identificado na década de 1990, exemplifica essa evolução ao explorar o protocolo ICMP para gerar tráfego massivo direcionado a uma vítima específica.

O impacto dos ataques DoS é amplamente documentado na literatura. Um estudo conduzido por Behal e Kumar (2017) enfatiza que tais ataques não apenas causam interrupções de serviço, mas também representam desafios significativos para a infraestrutura de rede devido à sua capacidade de explorar múltiplas vulnerabilidades, incluindo configurações incorretas de dispositivos e protocolos de rede obsoletos. Entre os diversos tipos de DoS, o ataque Smurf destaca-se por sua simplicidade de execução e capacidade de amplificação, sendo um exemplo clássico de como ataques que podem causar interrupções severas.

2.2 O Ataque Smurf

O ataque Smurf foi descrito pela primeira vez na década de 1990, explorando

o protocolo ICMP, que é usado principalmente para diagnósticos e mensagens de controle em redes IP. Este ataque aproveita configurações de rede inadequadas, como a capacidade de dispositivos responderem a solicitações ICMP Echo Request enviadas para endereços de broadcast (Cardoso, et al., 2018). Isso resulta em uma amplificação significativa do tráfego direcionado ao alvo, tornando o ataque especialmente eficaz.

O ataque Smurf utiliza pacotes ICMP Echo Request com endereços de origem falsificados, enviados para endereços de broadcast de redes intermediárias. Os dispositivos nessas redes respondem às solicitações, direcionando as respostas para a vítima, que é inundada com tráfego inesperado, resultando em degradação ou interrupção dos serviços. Essa técnica aproveita a amplificação proporcionada pelas respostas múltiplas dos hosts da rede intermediária.

Embora várias contramedidas tenham sido desenvolvidas, incluindo o bloqueio de pacotes ICMP Echo em roteadores e firewalls, estudos mostram que redes mal configuradas estão suscetíveis a ataques Smurf (Cardoso, et al., 2018). Essa persistência se deve em parte à expansão de redes heterogêneas, onde dispositivos IoT frequentemente utilizam configurações padrão que podem ser exploradas por atacantes.

2.3 Detecção e Mitigação de Ataques Smurf

Diversas abordagens têm sido propostas para detectar e mitigar ataques Smurf e outros baseados em ICMP. Uma estratégia comum é a filtragem de pacotes ICMP em roteadores e firewalls, impedindo que pacotes maliciosos alcancem a rede interna. Além disso, técnicas de aprendizado de máquina têm sido exploradas para identificar padrões anômalos de tráfego associados a esses ataques. Por exemplo, estudos recentes aplicaram algoritmos de aprendizado profundo para detectar ataques DDoS em redes definidas por software, demonstrando eficácia na identificação de tráfego malicioso (SHAHZEB, 2020).

Apesar dos avanços, as metodologias atuais enfrentam desafios significativos. A filtragem de pacotes pode resultar em falsos positivos, bloqueando tráfego legítimo, enquanto soluções baseadas em aprendizado de máquina

requerem conjuntos de dados extensivos e podem não generalizar bem para novos tipos de ataques (SINGH, 2020). Além disso, a implementação de tais soluções em redes de grande escala pode ser complexa e demandar recursos significativos.

2.4 Lacunas na Literatura e Justificativa da Pesquisa

Embora os avanços na detecção de ataques Smurf sejam evidentes, há lacunas significativas que precisam ser preenchidas. As principais limitações incluem:

- **Alta Incidência de Falsos Positivos:** Muitas abordagens existentes, especialmente as baseadas em heurísticas, geram alarmes falsos que podem sobrecarregar administradores de rede.
- **Falta de Adaptação a Redes Heterogêneas:** Dispositivos IoT e redes modernas introduzem complexidade adicional, dificultando a implementação de soluções universais.
- **Dependência de Dados de Treinamento:** Métodos baseados em aprendizado de máquina muitas vezes dependem de dados históricos, que podem não refletir padrões de ataque emergentes.

Dada essas lacunas, este estudo propõe um modelo de detecção baseado na análise de pacotes ICMP, com foco em reduzir falsos positivos e melhorar a adaptabilidade a diferentes configurações de rede. Além disso, ao testar o modelo em cenários simulados, busca-se fornecer uma solução prática e escalável para ambientes reais.

3. MATERIAL E MÉTODOS

3.1 Cenário Experimental

Para a realização deste estudo, foi criado um ambiente experimental utilizando máquinas virtuais para simular redes reais e cenários de ataque Smurf. As configurações e ferramentas utilizadas foram projetadas para permitir a implementação, teste e validação do modelo de detecção.

3.1.1 Configuração das Máquinas Virtuais

Foram utilizadas duas máquinas virtuais principais:

1. Máquina de Ataque:

- **Sistema Operacional:** Ubuntu (versão 24.04)
- **Função:** Simular o envio de pacotes ICMP maliciosos com endereços de origem falsificados para endereços de broadcast.

2. Máquina de Detecção:

- **Sistema Operacional:** Ubuntu (versão 24.04)
- **Função:** Hospedar o algoritmo de detecção e monitorar o tráfego de rede em busca de anomalias.

Além disso, o ambiente foi configurado utilizando o VirtualBox, com a seguinte configuração:

- **CPU:** 2 núcleos.
- **Memória RAM:** 4 GB.
- **Rede:** Modo de rede interna para garantir o isolamento do ambiente e controle total do tráfego.

3.2 Ferramentas Utilizadas

3.2.1 Linguagem de Programação e Bibliotecas

- **Linguagem:** Python, devido à sua versatilidade e suporte para bibliotecas específicas de análise de tráfego.

- **Bibliotecas:**

- **Scapy (versão 2.5.0):** Utilizada para capturar e analisar pacotes ICMP em tempo real.
- **smtplib:** Empregada para enviar notificações por e-mail em caso de detecção de ataques.

3.2.2 Ferramentas de Teste:

- **Nmap:** Ferramenta de escaneamento de rede utilizada para verificar a conectividade e a atividade dos hosts antes do início dos ataques.
- **Tcpdump:** Empregado para capturar pacotes ICMP na máquina vítima, permitindo a validação do tráfego gerado pelo ataque.

3.3 Configuração dos Testes Simulados

Os testes foram realizados para simular ataques Smurf e validar a capacidade do modelo de detecção em identificar pacotes maliciosos. A configuração dos testes incluiu os seguintes passos:

1. Inicialização do Ambiente:

- A máquina atacante foi configurada para enviar pacotes ICMP Echo Request com spoofing de endereço de origem, destinados a um endereço de broadcast.
- A máquina de detecção foi configurada para monitorar o tráfego de rede em tempo real.

2. Execução do Ataque:

- Utilizou-se um script no Kali Linux para enviar pacotes ICMP em modo inundação, simulando um ataque Smurf por 60 segundos.
- O comando: **sudo tcpdump -i eth0** foi utilizado na máquina vítima para validar a chegada dos pacotes ICMP.

3. Captura e Análise:

- O modelo desenvolvido na máquina de detecção capturou pacotes em tempo real e registrou padrões de tráfego anômalo.

3.4 Algoritmo de Detecção

O algoritmo de detecção foi projetado para identificar anomalias no tráfego ICMP, focando em padrões característicos de ataques Smurf.

FUNÇÃO detectar_ataque_smurf

INÍCIO

// Inicializar estruturas de dados

DICIONÁRIO icmp_echo_requests ← {}

DICIONÁRIO icmp_echo_replies ← {}

ENDEREÇO_BROADCAST ← "255.255.255.255"

LIMIAR_REQUESTS ← 100

LIMIAR_REPLIES ← 100

// Capturar pacotes ICMP em tempo real

PARA cada pacote EM capturar_pacotes():

// Verificar tipo de pacote

SE pacote.tipo == "ICMP_ECHO_REQUEST" ENTÃO

// Verificar destino de broadcast

SE pacote.destino == ENDEREÇO_BROADCAST ENTÃO

AUMENTAR icmp_echo_requests[pacote.origem] EM 1

SENÃO SE pacote.tipo == "ICMP_ECHO_REPLY" ENTÃO

AUMENTAR icmp_echo_replies[pacote.destino] EM 1

// Verificar padrões de ataque

SE verificar_ataque icmp_echo_requests, icmp_echo_replies,

LIMIAR_REQUESTS, LIMIAIR_REPLIES) ENTÃO

ENVIAR_ALERTA("Ataque Smurf Detectado!")

RESETAR icmp_echo_requests

RESETAR icmp_echo_replies

FIM PARA

FIM

FUNÇÃO capturar_pacotes

INÍCIO

ENQUANTO capturando:

pacote ← capturar_pacote_rede()

RETORNAR pacote

FIM ENQUANTO

FIM

FUNÇÃO verificar_ataque

INÍCIO

PARA cada origem EM icmp_echo_requests:

SE icmp_echo_requests[origem] > LIMIAIR_REQUESTS E
icmp_echo_replies[origem] > LIMIAIR_REPLIES ENTÃO

RETORNAR VERDADEIRO

FIM PARA

RETORNAR FALSO
FIM

FUNÇÃO enviar_alerta

INÍCIO

// Envia notificação ao administrador de rede

IMPRIMIR mensagem

ENVIA_MENSAGEM_EMAIL(mensagem)

FIM

3.4.1 Descrição das Principais Funcionalidades

1. Captura de Pacotes:

- A função capturar_pacotes monitora o tráfego de rede em tempo real, capturando pacotes ICMP.

2. Armazenamento de Dados:

- Os pacotes ICMP Echo Request e Echo Reply são armazenados em dicionários para rastrear o número de pacotes recebidos por origem e destino.

3. Verificação de Ataque:

- A função verificar_ataque compara os contadores de pacotes ICMP com os limiares predefinidos. Se o número de pacotes exceder os limiares, o ataque é detectado.

4. Notificação:

- Quando um ataque é detectado, a função enviar_alerta gera um alerta para o administrador de rede e reinicia os contadores.

3.5 Critérios de Avaliação

Os testes foram avaliados com base em métricas de desempenho, considerando:

1. Taxa de Verdadeiro Positivo (TVP):

- Proporção de ataques Smurf corretamente detectados pelo modelo.
- Fórmula:

$$TVP = \frac{\text{Detecções Verdadeiras}}{\text{Ataques Reais}}$$

2. Taxa de Falso Positivo (TFP):

- Proporção de tráfego legítimo erroneamente identificado como ataque.
- Fórmula:

$$TFP = \frac{Falso\ Positivos}{Tráfego\ Legítimo}$$

3. Tempo de Resposta:

- Tempo necessário para o algoritmo identificar e alertar sobre um ataque, medido desde a captura inicial do pacote até a geração do alerta.

4. RESULTADOS E DISCUSSÃO

4.1 Resultados Obtidos nos Cenários Simulados

Os testes foram conduzidos em um ambiente controlado, utilizando máquinas virtuais configuradas para simular redes reais, conforme descrito anteriormente. O modelo de detecção foi avaliado quanto à sua eficácia em identificar ataques Smurf, com os seguintes indicadores:

4.1.1 Taxas de Detecção

- **Taxa de Verdadeiro Positivo (TVP):**

A TVP foi medida como a proporção de ataques Smurf corretamente identificados pelo modelo. Nos testes realizados, o modelo alcançou uma taxa de 89%, indicando uma alta eficácia na detecção de ataques. Isso demonstra a capacidade do modelo de capturar padrões característicos de pacotes ICMP maliciosos enviados para endereços de broadcast.

- **Taxa de Falso Positivo (TFP):**

A TFP foi avaliada para verificar a incidência de tráfego legítimo erroneamente classificado como ataque. Durante os testes, a TFP foi de 7%, o que representa uma margem aceitável, mas indica espaço para melhorias na filtragem de pacotes legítimos.

4.1.2 Tempo de Resposta

O tempo médio de resposta do modelo, desde a captura do primeiro pacote até a geração de um alerta de ataque, foi de 1,2 segundos. Este resultado é satisfatório para detecção em tempo real, demonstrando que o modelo pode ser

aplicado em redes que exigem alta reatividade.

4.2 Discussão das Limitações

Apesar dos resultados promissores, o modelo de detecção apresenta algumas limitações que precisam ser consideradas:

1. Dependência de Configurações de Rede:

- O desempenho do modelo depende de redes configuradas para permitir o tráfego ICMP, o que pode variar em diferentes ambientes. Redes que já bloqueiam pacotes ICMP de broadcast podem reduzir a utilidade do modelo.

2. Ambiente Controlado:

- Os testes foram realizados em cenários simulados, onde o tráfego é controlado e previsível. Em redes reais, com padrões de tráfego mais complexos, o desempenho do modelo pode ser impactado.

3. Sensibilidade a Limiar de Detecção:

- A definição dos limiares de ICMP Echo Request e Echo Reply influencia diretamente as taxas de detecção. Limiar inadequado pode resultar em aumento de falsos positivos ou na incapacidade de detectar ataques.

4. Impacto do Volume de Tráfego:

- Em redes de alta densidade, o modelo pode enfrentar dificuldades para processar grandes volumes de tráfego em tempo real, exigindo ajustes em sua implementação para melhorar a escalabilidade.

Os resultados obtidos validam a eficácia do modelo proposto em cenários simulados, destacando sua precisão e capacidade de detecção em tempo real. O modelo se mostra competitivo, especialmente em relação à redução de falsos positivos. No entanto, as limitações identificadas apontam para a necessidade de testes adicionais em redes reais e de melhorias na adaptabilidade e escalabilidade do modelo.

Este trabalho apresenta uma solução prática para detecção de ataques Smurf, reforçando a importância da análise direta de pacotes ICMP como uma

abordagem eficaz e acessível para a segurança de redes. Futuros desenvolvimentos incluirão a aplicação do modelo em redes mais complexas e a integração com sistemas automáticos de mitigação.

5. CONSIDERAÇÕES FINAIS

Este estudo apresentou o desenvolvimento e avaliação de um modelo de detecção para ataques Smurf, baseado na análise de pacotes ICMP. Os resultados obtidos em cenários simulados demonstraram que o modelo é eficaz na identificação de padrões maliciosos associados a este tipo específico de ataque de negação de serviço (DoS), alcançando uma taxa de verdadeiro positivo de 89% e um tempo de resposta de 1,2 segundos. Esses indicadores refletem a capacidade do modelo de operar em tempo real, proporcionando uma detecção precisa e reativa.

A principal contribuição deste trabalho reside na proposta de um modelo acessível e eficiente para segurança de redes, que utiliza bibliotecas amplamente disponíveis, como a Scapy, para capturar e analisar tráfego de rede. Diferentemente de metodologias baseadas em aprendizado de máquina, que frequentemente requerem grandes volumes de dados históricos para treinamento, o modelo proposto focasse em características intrínsecas dos pacotes ICMP, reduzindo complexidade e custo de implementação. Isso reforça a relevância prática e acadêmica do estudo, ao oferecer uma solução viável para redes que enfrentam desafios de configuração inadequada e tráfego malicioso.

Embora os resultados tenham sido promissores, algumas limitações foram identificadas, destacando áreas para futuras melhorias. A redução de falsos positivos, atualmente em 7%, será uma prioridade para tornar o modelo mais robusto em cenários com padrões de tráfego legítimos mais variáveis. Além disso, a integração com sistemas automáticos de mitigação pode aumentar a eficiência do modelo, permitindo que ele não apenas detecte ataques, mas também atue ativamente para neutralizá-los.

Avanços futuros inclui a aplicação do modelo em redes mais complexas e heterogêneas, como redes empresariais e ambientes que integram dispositivos IoT. Esse tipo de cenário introduz novos desafios devido ao aumento da densidade e diversidade de tráfego, mas também amplia a aplicabilidade do modelo em situações reais.

REFERÊNCIAS

Ataque de negação de serviço, Disponível em: <https://pt.wikipedia.org/wiki/Ataque_de_nega%C3%A7%C3%A3o_de_servi%C3%A7o> Acesso em 10 novembro. 2024.

BEHAL, Sunny. KRISHAN, Kumar. '**Detection of DDoS attacks and flash events using information theory metrics–An empirical investigation**'. Disponível em: <<http://dx.doi.org/10.1016/j.comcom.2017.02.003>> Acesso em 10 out. 2024.

CARDOSO, Adeilson Marques da Silva et al. **CEPIDS: Um IDS baseado no Processamento de Eventos Complexos para Internet de Coisas.** 2018. Disponível em: <<https://tedebc.ufma.br/jspui/bitstream/tede/2360/2/Adeilson%20Marques.pdf>> Acesso em: 25 out. 2024.

HAIDER, S. AKHUNZADA, A. MUSTAFA, L. BHARAT, T. P. FERNANDEZ, A. RAYMOND, K. C. **A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks.** Disponível em: <https://ieeexplore.ieee.org/document/9016053?utm_source=chatgpt.com> Acesso em: 18 set. 2024.

SINGH, P. S.; BEHAL. S.; BHATIA, S. **Detection of DDoS Attacks using Machine Learning Algorithms.** Disponível em: <<https://ieeexplore.ieee.org/document/9083716>> Acesso em: 28 out. 2024.

STEVE, Yannis N. F.; KENGNE, V. T.; VELEMPINI, M. **Federated Learning Based DDoS Attacks Detection in Large Scale Software-Defined Network,** 2024. Disponível em: <<https://ieeexplore.ieee.org/document/10705345/authors#authors>> Acesso em: 01 nov. 2024.