



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

ALEXANDRE GOMES DANIEL

**MODELO DE DETECÇÃO DE INTRUSÃO POR BRUTE FORCE UTILIZANDO
SCAPY E RASPBERRY PI**

**ARAGUATINS – TO
2024**

ALEXANDRE GOMES DANIEL

**MODELO DE DETECÇÃO DE INTRUSÃO POR BRUTE FORCE UTILIZANDO
SCAPY E RASPBERRY PI**

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

Orientador: Prof. Me. Adeilson Marques da Silva
Cardoso

Coorientador: Prof. Me. Ancelmo Frank Coelho
Castro

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

D184m Daniel, Alexandre Gomes
Modelo de Detecção de Intrusão por Brute Force Utilizando
Scapy e Raspberry Pi / Alexandre Gomes Daniel. – ARAGUATINS,
TO, 2024.
23 f. : 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
Coorientador: Me. Ancelmo Frank Coelho Castro

1. Detecção de Ataque. 2. Brute Force. 3. Scapy. I. Cardoso,
Adeilson Marques da Silva. II. Castro, Ancelmo Frank Coelho. III.
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).



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

FOLHA DE APROVAÇÃO

TÍTULO: MODELO DE DETECÇÃO DE INTRUSÃO POR BRUTE FORCE UTILIZANDO SCAPY E RASPBERRY PI

AUTOR: **ALEXANDRE GOMES DANIEL**

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 21 de junho de 2024.

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

PROF. DR. RAMÁSIO FERREIRA DE MELO
Primeiro avaliador

PROF. ME. ROGÉRIO PEREIRA DE SOUSA
Segundo avaliador



Documento assinado eletronicamente por **Adeilson Marques da Silva Cardoso, Servidor**, em 21/06/2024, às 15:26, 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 **Ramasio Ferreira de Melo, Servidor**, em 21/06/2024, às 15:26, 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 **Rogério Pereira de Sousa, Servidor**, em 21/06/2024, às 15:27, 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.iftto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2416552** e o código CRC **A31C398E**.

AGRADECIMENTOS

Agradeço, primeiramente a Deus, por colocar tudo em seu devido lugar.

A meus pais e meu irmão, que me auxiliaram nos momentos de dificuldade durante esse tempo que entrei na faculdade.

A minha tia Claudete que me apoiou e me recebeu em sua casa de braço abertos.

Aos meus professores, principalmente aos professores Adeilson que me propôs este trabalho. Ao professor Ancelmo que me auxiliou durante a criação e correção deste projeto.

RESUMO

O artigo apresenta uma solução de baixo custo para a detecção de ataques de força bruta em redes, utilizando o Raspberry Pi como um sensor de rede. O Raspberry Pi é empregado para monitorar o tráfego de rede e identificar possíveis ataques, oferecendo um mecanismo de defesa eficaz para redes de pequeno e médio porte. Utilizando a ferramenta scapy para captura e análise de pacotes de rede, e simulando ataques com a ferramenta Hydra em senhas de SSH, os testes demonstraram que o Raspberry Pi foi capaz de detectar com sucesso os ataques de força bruta, gerando alertas em tempo real e registrando os endereços IP dos invasores. Além disso, o artigo propõe o uso de um servidor de e-mail para envio de alertas, permitindo que os administradores de rede possam agir rapidamente para bloquear os ataques. Essa solução demonstra que, mesmo com poder computacional reduzido, o Raspberry Pi pode ser uma ferramenta eficaz na proteção de redes contra ataques de força bruta, reforçando sua utilidade em ambientes de IoT que exigem defesas rápidas e precisas.

Palavras-chave: Detecção de ataques, Brute Force, Scapy, Raspberry Pi.

RESUMO EM LÍNGUA ESTRANGEIRA

The article presents a low-cost solution for detecting brute force attacks on networks, using the Raspberry Pi as a network sensor. The Raspberry Pi is used to monitor network traffic and identify possible attacks, offering an effective defense mechanism for small and medium-sized networks. Using the scapy tool to capture and analyze network packets, and simulating attacks with the Hydra tool on SSH passwords, the tests demonstrated that the Raspberry Pi was able to successfully detect brute force attacks, generating real-time alerts and recording the IP addresses of attackers. Furthermore, the article proposes the use of an email server to send alerts, allowing network administrators to act quickly to block attacks. This solution demonstrates that, even with reduced computing power, the Raspberry Pi can be an effective tool in protecting networks against brute force attacks, reinforcing its usefulness in IoT environments that require fast and accurate defenses.

Keywords: Attack Detection, Brute Force, Scapy, Raspberry Pi

LISTA DE ILUSTRAÇÕES

- Figura 1 - Ataque de Força Bruta16
- Figura 2 - Bloqueio de Ataque de Força Bruta21
- Figura 3 - Análise e captura dos pacotes com destino a porta 2222
- Figura 4 - Contagem dos pacotes com destino a porta 2222
- Figura 5 - Criação e checagem do registro23
- Figura 6 - Criando regras de Firewall23
- Figura 7 - Envio do e-mail de alerta para o administrador24

LISTA DE SIGLAS

SSH	SECURE SHELL
TCP	TRANSMISSION CONTROL PROTOCOL
IP	INTERNET PROTOCOL
SMTP	SIMPLE MAIL TRANSFER PROTOCOL

Sumário

1 INTRODUÇÃO	15
2. REFERENCIAL TEÓRICO.....	16
2.1 Segurança.....	16
2.2 Ataques de força bruta	17
2.3 Raspibarry pi	18
2.4 Ferramenta hydra.....	18
2.5 Ferramenta scapy	19
3. METODOLOGIA	19
4. RESULTADOS E DISCUSSÕES	21
5. CONCLUSÃO	25
REFERÊNCIAS.....	26

1 INTRODUÇÃO

Ao longo dos anos, a tecnologia progrediu rapidamente, penetrando cada vez mais na vida quotidiana das pessoas e mudando profundamente a forma como a sociedade funciona. Inserido num mundo de crescente autonomia, este contexto facilita a transmissão de dados, muitos dos quais são altamente sensíveis. No entanto, esta evolução também resultou em um aumento significativo e contínuo de tentativas de ataques cibercriminosos, resultando no atual cenário desafiado os processos tecnológicos que estão em constantes mudanças.

Compreender os mecanismos subjacentes aos ciberataques é fundamental para tanto a segurança de cada utilizador presente dentro da sociedade que utiliza a tecnologia durante o decorrer do dia a dia ou para guardar seus dados mantendo resiliência de redes informáticas inteiras. Tais ataques podem penetrar em qualquer rede, seja ela empresarial ou individual, e atrair a atenção de invasores que buscam identificar seus alvos e obter informações confidenciais. Os ataques cibernéticos podem assumir muitas formas e técnicas. Em alto nível, esses ataques geralmente coletam dados da vítima, preparando o próximo estágio de ataques que exploram esses dados (Jonghoon, et al. 2021). Por outro lado, também existem variantes de ataques que exploram vulnerabilidades até então desconhecidas em sistemas e redes para quebrar barreiras de segurança e torná-los mais vulneráveis a novos ataques (Kamau, et al. 2021).

Um ataque de força bruta ou “brute force attack” é baseado em uma abordagem de tentativa e erro. Esse tipo de ataque aciona uma solicitação de acesso com possíveis valores, como métodos e chaves de acesso, prováveis combinações de conta e senha de acesso de um sistema e assim por diante. O objetivo é romper a barreira de segurança e ter acesso aos dados de interesse. Para atingir esse objetivo, o invasor cria uma lista contendo diversas combinações possíveis de caracteres formados por letras maiúsculas e minúsculas, números, símbolos, originando o chamamos de “dicionário”. Um agente malicioso testa diversas combinações desses dicionários até encontrar a ordem correta. Milhares dessas combinações podem ser testadas a cada segundo conforme pode ser verificado na Figura 1.

Figura 1 - Ataque de Força Bruta



Fonte: próprio autor

Compreender as nuances destas táticas é fundamental para fortalecer as suas defesas digitais e proteger dados sensíveis num mundo onde a sofisticação dos ataques cibernéticos continua a evoluir. Conhecer as táticas utilizadas pelos cibercriminosos pode ajudar a construir barreiras mais fortes e estratégias de resposta mais eficazes para garantir a segurança da informação num ambiente virtual cada vez mais complexo e conectado.

Diante desse cenário, torna-se imperativo desenvolver e implementar soluções eficazes para mitigar os riscos associados aos ataques de força bruta. A utilização de dispositivos de baixo custo, como o Raspberry Pi, para monitoramento e detecção desses ataques oferece uma abordagem viável e eficiente. Sendo o Raspberry Pi uma placa do tamanho de cartão de crédito utilizada amplamente em projetos de pequeno e médio porte juntamente, em alguns casos, com sensores ligados a ela. Este artigo explora a aplicação do Raspberry Pi como um sensor de rede, demonstrando sua capacidade de identificar e alertar sobre tentativas de força bruta em tempo real, fornecendo uma camada adicional de segurança para redes de pequeno e médio porte. Ao integrar ferramentas de análise de tráfego e sistemas de alerta, nossa abordagem visa não apenas detectar ataques, mas também permitir respostas rápidas e coordenadas, fortalecendo a resiliência das redes contra ameaças cibernéticas contínuas.

2. REFERENCIAL TEÓRICO

2.1 Segurança

A segurança de uma rede é fundamental para garantir a tranquilidade dos usuários ao utilizá-la. A manutenção e a verificação constante de possíveis ameaças que possam estar presentes ou que possam penetrar na rede são inquestionáveis.

Com o passar dos anos, os invasores de redes de computadores têm adquirido habilidades cada vez mais avançadas, utilizando essas competências para explorar vulnerabilidades desconhecidas e contornar as soluções de segurança (Kamau, et al. 2021).

Com o desenvolvimento dessas habilidades, novas táticas são criadas para superar a proteção de um sistema, resultando no desenvolvimento de novas formas de defesa. Em contrapartida, também são criados novos métodos para contornar essa segurança imposta para proteger a vítima (Nakamura e Geos, pág. 25). Portanto, é preciso entender que a maioria dos ataques se baseia em vulnerabilidades existentes devido a alguma falha no projeto, falta de implementação de protocolos, regras de firewall, erros de configuração e administração dos recursos operacionais (Nakamura e Geos, pág. 26).

Segundo Nakamura e Geos, apesar de que a maioria dos ataques registrados podem ser oportunistas, existem também os ataques direcionados para uma vítima ou um grupo de vítimas. Esses ataques direcionados tentam ser mais perigosos pois envolve um estudo mais aprofundado daquele sistema de defesa de modo a executar e explorar o elo mais fraco presente no sistema tendo maiores prejuízos pois como não são feitos de maneiras aleatórias tendem a ser mais agressivos. Quanto mais agressivo for o ataque maior será o nível de esforço para tentar detê-lo e consequentemente maiores perdas.

2.2 Ataques de Força Bruta

O ataque de força bruta é um dos principais ataques usados para intrusão de redes de computadores por sua maneira simplista de como acontece a tentativa de conseguir quebrar a segurança presente para a proteção da vítima. Outra coisa a se destacar que

os ataques de força bruta estão se tornando mais difíceis de detectar com sucesso em nível de rede devido à crescente onipresença de redes de alta velocidade e ao aumento do volume e da criptografia do tráfego de rede (Kamau, et al. 2021).

Mesmo com as dificuldades de detecção deste tipo de ataque, com os avanços e criação de ferramentas utilizadas para a segurança da rede de computadores,

pode detectar indicadores ou sinais que estão acontecendo o processo de intrusão dentro da rede.

Vários sinais podem ser interpretados como indicadores de um ataque de força bruta. Entre eles, várias tentativas de login com falha do mesmo endereço IP; logins com várias tentativas de nome de usuário do mesmo endereço IP; logins para uma única conta de muitos endereços IP diferentes; tentativas de login com falha de nomes de usuário e senhas em ordem alfabética; logins com uma URL de referência do e-mail ou cliente IRC de alguém; consumo excessivo de largura de banda ao longo de uma única sessão e um grande número de falhas de autenticação. (Kamau, et al. 2021)

Compreender como funciona e são realizados os ataques de força bruta, como também possíveis soluções e abordagens empregadas é de suma importância para que novas pesquisas e contribuições possam ser geradas para a proteção e segurança da informação dos sistemas computacionais (Diorio, et al. 2019).

2.3 Raspberry Pi

O Raspberry Pi desempenha um papel fundamental como monitor de rede, acompanhando os dados que são trafegados. Para simplificar, o Raspberry Pi é um minicomputador do tamanho aproximado de um cartão de crédito desenvolvido pela Raspberry Pi Foundation (Jolles, pág. 1564). Ele funciona como um dispositivo portátil equipado com um processador de arquitetura ARM e sistemas operacionais baseados em Linux. Um ponto importante a destacar é que o Raspberry Pi é configurado usando Python, que é a linguagem oficial do dispositivo e possui um ambiente de desenvolvimento integrado para essa linguagem.

Esta ferramenta é amplamente utilizada em projetos que requerem um dispositivo de processamento de baixo custo. Sua versatilidade e acessibilidade a tornam uma escolha popular em diversas áreas que necessitam de tal equipamento (Jolles, pág. 1563).

2.4 Ferramenta Hydra

Hydra é uma ferramenta poderosa utilizada para realizar ataques de força bruta em sistemas ou máquinas, com o objetivo de descobrir senhas. Ela emprega um modelo de ataque simplista, que consiste em enviar requisições para realizar testes utilizando uma lista de senhas pré-definidas até encontrar a senha correta.

Ao realizar uma tentativa ataque usando a ferramenta Hydra, é necessário configurar alguns parâmetros. Primeiramente será necessário o nome de usuário da máquina alvo, o caminho para a lista de possíveis senhas que a Hydra usará no ataque, especificar o tipo de protocolo que a Hydra deve usar para se comunicar com a máquina alvo além de poder acompanhar o progresso do ataque usando.

Depois de configurar esses parâmetros, o comando para iniciar o ataque com a Hydra ficaria algo parecido com:

```
hydra -l <nome de usuário> -P <caminho da lista de senhas> <endereço ip da vítima>  
<protocolo> (Manual Hydra)
```

É importante notar que, embora a Hydra seja uma ferramenta poderosa, seu uso pode ser ilegal dependendo das circunstâncias. Portanto, ela deve ser usada com responsabilidade e apenas para fins legítimos, como testes de penetração autorizados ou auditorias de segurança.

2.5 Ferramenta Scapy

Scapy é uma poderosa ferramenta de manipulação de pacotes baseada em Python. Ela tem a capacidade de codificar, decodificar, enviar e combinar remetentes e destinatários de pacotes de maneira interativa. Devido à sua capacidade de identificar falhas no sistema de segurança que normalmente passam despercebidas pelos firewalls, Scapy é considerada mais eficaz do que muitos firewalls tradicionais (Shipra e Nitin, 2018).

A ferramenta foi criada por Philippe Biondi com o objetivo de desenvolver uma solução robusta capaz de realizar várias tarefas simultaneamente e responder a uma variedade de solicitações. A implementação de Scapy é feita através de instâncias de classes, seguindo o paradigma da Orientação a Objetos. Isso significa que os pacotes são implementados como objetos, permitindo a instanciação das classes e pacotes presentes dentro da ferramenta para manipulação de pacotes.

Além disso, Scapy é altamente flexível e personalizável, permitindo aos usuários ajustarem suas funcionalidades de acordo com suas necessidades específicas. Isso torna Scapy uma ferramenta valiosa não apenas para a detecção de

vulnerabilidades de segurança, mas também para uma ampla gama de aplicações como testes de segurança de redes, exploração de dados e desenvolvimento de protocolos personalizados.

3. METODOLOGIA

O desenvolvimento do projeto baseou-se em pesquisas de artigos acadêmicos relevantes e na utilização de tutoriais para aprender e configurar as máquinas e o sistema de detecção. Além disso

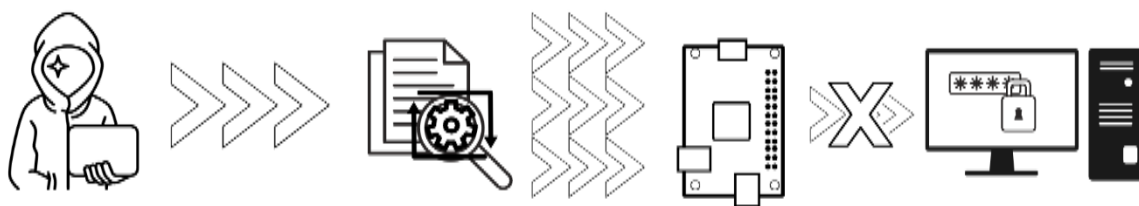
A configuração da rede virtualizada consiste em duas máquinas virtuais, sendo uma delas utilizando Kali Linux e a outra o Ubuntu 22.04 LTS, cada uma desempenhando uma função específica no experimento. A primeira máquina virtual foi preparada com software Hydra na versão 9.5 e foi capaz de emular um ataque de força bruta. Enquanto isso, uma segunda máquina virtual foi configurada para executar um serviço que exigia autenticação SSH, com suporte adicional para Scapy, uma ferramenta para captura e análise aprofundada de tráfego de rede estando na versão 2.5.0. O núcleo do experimento foi o desenvolvimento de algoritmos de análise de tráfego projetados usando a linguagem de programação Python. Este algoritmo é usado para identificar padrões suspeitos que aparecem nos fluxos de tráfego. O Raspberry Pi utilizado sendo a versão 3 model B de 1 gb de RAM utilizando sua distribuição oficial Linux, o Raspberry Pi OS.

Nos concentramos no comportamento do tráfego para detectar atividades anômalas. O objetivo principal era identificar o tráfego que se desviava das normas tradicionais, reconhecendo sintomas como múltiplas tentativas de autenticação em intervalos curtos. Esta abordagem metódica e tecnicamente avançada permitiu simular cenários de ataque e implementar sistemas de análise de tráfego altamente sensíveis. Uma combinação de software especializado e algoritmos personalizados nos permite rastrear atividades anômalas e potencialmente maliciosas. Esta análise aprofundada do tráfego, apoiada por ferramentas de ponta e programação inteligente, aumenta a nossa capacidade de detectar e combater ameaças cibernéticas instantaneamente, aumentando assim a segurança da rede em questão.

Com base na análise cuidadosa desses padrões de comportamento anômalos, o sistema demonstra a capacidade de identificar cuidadosamente possíveis possibilidades de ataque. Uma vez feita essa identificação, o sistema adota uma abordagem proativa e implementa mecanismos de bloqueio temporário que são

eficazes por um curto período de tempo. Esta medida de contenção visa neutralizar e conter tentativas de intrusão, limitando o acesso não autorizado. Porém, em cenários onde persistem ataques maliciosos, o sistema aumenta sua postura de defesa. A Resposta Adaptativa reativa a ação de bloqueio para proteger melhor a máquina alvo. Durante esta fase, são tomadas medidas mais rigorosas, como rejeitar imediatamente todas as solicitações enviadas ao computador alvo (Figura 2). Esta abordagem ponta a ponta não só garante a integridade do ambiente digital, mas também a operação contínua e ininterrupta dos sistemas envolvidos. Portanto, ao abordar este processo de detecção e resposta, o sistema está mais apto a combater e mitigar ameaças cibernéticas. Seu desempenho estratégico ajuda a impulsionar ambientes virtuais seguros onde a confidencialidade, a disponibilidade e a confiabilidade continuam sendo pilares fundamentais.

Figura 2 - Bloqueio de Ataque de Força Bruta



Fonte: próprio autor

4. RESULTADOS E DISCUSSÕES

Nesta seção, discutiremos sobre o resultado do modelo de detecção de ataque de força bruta utilizando a biblioteca scapy e o Raspberry Pi analisando a sua eficácia em proteger a vítima de uma possível tentativa de intrusão utilizando brute force.

O computador atacante envia os requerimentos de conexão para a vítima configurada com o IP 172.168.53.28 na porta padrão do SSH, porta 22. Ao ocorrer o envio dos requerimentos para esta porta, o modelo de detecção analisava cada pacote que estará passando na rede durante sua ativação com a função *sniff()*, usada para “farejar” os pacotes presentes na rede, filtrando para análise mais detalhada os pacotes do protocolo de rede TCP com destino na porta 22 (Figura 3).

Figura 3 - Análise e captura dos pacotes com destino a porta 22

```
# Função para capturar pacotes
funcao capturar_pacotes():
    tentar:
        farejar(filtro="tcp na porta 22", prn=detectar_forca_bruta)
    exceto Interrupção_do_Teclado:
        imprimir("Captura de pacotes interrompida pelo usuário.")

capturar_pacotes()
```

Fonte: próprio autor

Após capturar o primeiro pacote aplicado no filtro os dados são enviados para uma função que checará os pacotes separando-os mais ainda para poder fazer uma checagem mais aprofundada. Posteriormente de fazer essas análises mais aprofundadas o programa inicia um contador de tempo a partir do horário descrito na máquina para ter uma base de quantos pacotes estarão passando pela rede com o objetivo da vítima em um curto prazo de tempo, como também um segundo contador que irá aumentar de acordo com a quantidade de pacotes filtrados transitando pela rede contendo como limites de 10 tentativas de acesso por minuto, levando em consideração que o acesso remoto será utilizado com a taxa de quantidades de erros digitada por pessoas (Figura 4).

Figura 4 - Contagem dos pacotes com destino a porta 22

```
# Função para detectar força bruta
funcao detectar_forca_bruta(pacote):
    tentar:
        se pacote_do_tipo(TCP) e pacote[TCP].porta_de_destino -> 22:
            i p = pacote[IP].src
            marcar_hora = tempo_atual()

# Ignora pacotes de IPs bloqueados
tentativas_autenticacao[ip].acrescentar(marcar_hora)
# Remova as tentativas de autenticação antigas do dicionário tentativas_autenticacao[ip] =
[t de t em tentativas_autenticacao[ip] se marcar_hora - t <= INTERVALO_DE_TEMPO]
```

Fonte: próprio autor

Antes de iniciar a tentativa de bloqueio, será verificado uma lista de IPs presentes em um arquivo chamado `ssh_bruteforce.log` e se ele está criado dentro do sistema, verificando se já aconteceu alguma outra tentativa de ataque do IP do invasor, caso não exista este arquivo ele será criado e irá guardar o IP do atacante para evitar

futuras tentativas de atacar a vítima (Figura 5)... Em seguida é mandado um comando de iptables para o firewall da vítima, contendo uma regra de entrada de dados recusando qualquer requerimento do IP atacante, notificando, posteriormente, se a regra de iptables caso sucedida (Figura 6).

Figura 5 - Criação e checagem do registro

```
# Configuração do registro
configurar_registro(filename='ssh_bruteforce.log', level=INFO, format='%
(asctime)s - %(message)s')
# Dicionário para rastrear as tentativas de autenticação por endereço IP
tentativas_autenticacao = criar_dicionario()
# Conjunto para rastrear IPs bloqueados
ips_bloqueados = criar_conjunto()
```

Fonte: próprio autor

Figura 6 - Criando regras de Firewall

```
# Registre no log
registrar_log(ip, tamanho(tentativas_autenticacao[ip]))
# Bloqueie o IP de origem e adicione-o à lista de IPs bloqueados
comando_iptables = "iptables -A INPUT -s {ip} -j DROP"
subprocesso.acionar(comando_iptables, shell=True, check=True)
adicionar_elemento(ips_bloqueados, ip)
imprimir(f"A regra iptables para bloquear {ip} foi criada com sucesso.")
```

Fonte: próprio autor

Como última etapa, será configurado uma parte do código para enviar um e-mail para o administrador da vítima, durante este processo o IP do atacante será transformado em um tipo de dado chamado de String, ou no python, str para que o IP seja transformado em texto evitando problemas de incompatibilidade durante o envio da mensagem. Será utilizado uma biblioteca já presente no python para enviar a mensagem pré-determinada via protocolo SMTP e ajustada pela biblioteca MineText, pois sem ela a quantidades de caracteres que podem ser utilizados para criar uma mensagem ou texto é drasticamente reduzida, além de poder alguns problemas de incompatibilidade de organização do conteúdo (Figura 6).

Figura 7 - Envio do e-mail de alerta para o administrador

```
# Envie um email de alerta
enviar_email(ip)
exceto Excecao como erro:
    imprimir(f"Ocorreu um erro")
# Função para enviar email
funcao enviar_email(ip):
    tentar:
# Configuração do servidor e credenciais
servidor = SMTP(dados)
servidor.starttls()
servidor.login(email e senha)
# Criação da mensagem
email_de_origem = "email"
email_de_destino = "email"
assunto = "Alerta de Ataque de Força Bruta SSH"
corpo = "<p>Possível ataque de força bruta detectado a partir de {ip}!</p>"
# Enviando o email
servidor.sendmail(email_de_origem, email_de_destino, mensagem)
# Encerrando a conexão
servidor.sair()
imprimir("Email de alerta enviado para {email_de_destino}")
exceto Excecao como e:
    imprimir(f"Erro ao enviar email: erro")
```

Fonte: próprio autor

5. CONCLUSÃO

Após a análise detalhada dos resultados obtidos com o modelo de detecção de intrusão de ataques de força bruta utilizando a biblioteca Scapy e o Raspberry Pi, pode-se concluir que a abordagem se mostrou funcional na proteção das redes de computadores contra ameaças desse tipo. A capacidade de analisar o tráfego de rede de forma rápida e eficiente, aliada à economia de recursos e custos proporcionada pelo uso do Raspberry Pi, destaca a viabilidade e o potencial dessa solução para redes de pequeno e médio porte.

No entanto, é importante ressaltar que, apesar dos benefícios apresentados, a configuração adequada dos servidores e máquinas utilizadas continua sendo fundamental. A verificação constante de possíveis falhas e a adoção de medidas de segurança adicionais são essenciais para mitigar o risco de intrusões, especialmente considerando a capacidade dos atacantes de explorar outras portas e alterar configurações padrão.

Como perspectiva para trabalhos futuros, sugere-se a adaptação e implementação desse modelo de detecção de ataques de força bruta para ambientes de Internet das Coisas (IoT). O crescente uso de dispositivos IoT em diversos contextos torna essencial a atenção à segurança desses dispositivos, a fim de evitar potenciais falhas que possam resultar no comprometimento de dados sensíveis. Portanto, estender essa abordagem para proteger dispositivos IoT pode contribuir significativamente para garantir a segurança e privacidade dos usuários.

REFERÊNCIAS

AMIJOYO, Tarisno. UMAR, Rusydi. YUDHANA, Anton. **Bruteforce In The Hydra Process And Telnet Service Using The Naïve Bayes Method**. Disponível em: <https://iocscience.org/ejournal/index.php/mantik/index>. Acesso em: 24 mai 2024.

DIORIO, Rafael F.; SERAFIM, Edivaldo; ALVES, Karlan R.; MEIRA, Matheus C. **Ataques de Força Bruta: Um Estudo Prático**. Disponível em: <https://lcv.fee.unicamp.br/images/BTSym-19/Papers/040.pdf>. Acesso em: 13 junho 2023.

JOLLES, Jolle W. **BOARD-SCALE APPLICATIONS OF THE RASPBERRY PI: A review and guide for biologists**. Disponível em: <https://besjournals.onlinelibrary.wiley.com/doi/epdf/10.1111/2041-210X.13652>. Acesso em: 21 jun 2024.

KHOA, Trieu. YI, Yang. **Artificial Intelligence-Based Password Brute Force Attacks**. Disponível em: <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1038&context=mwais2018>. Acesso em: 01 agosto 2023.

MAJUMDAR, Aayush; RAJ, Shruti; SUBBULAKSHMI, T. **ARP Poisoning Detection and Prevention using Scapy**. Disponível em: <https://iopscience.iop.org/article/10.1088/1742-6596/1911/1/012022>, Acesso em: 24 mai 2024.

MITULGIRI, H. Gauswami; KIRAN, R. Trivedi. **Implementation of Machine Learning for Gender Detection using CNN on Raspberry Pi Platform**. Disponível em: <https://ieeexplore.ieee.org/document/8398872>. Acesso em: 25 mai 2024.

MOHD, Yazid I. REZA Firsandaya M. SITI, Nurmaini. NIZAR, Alsharif. RAHMAT, Budiarto. **Investigating Brute Force Attack Patterns in IoT Network**. Disponível em: <https://www.hindawi.com/journals/jece/2019/4568368/>. Acesso em: 01 agosto 2023.

PARK, Jeonghoon; KIM, Junsu; GUPTA, B. B.; PARK, Namje. **Network Log-Based SSH Brute-Force Attack Detection Model**. Disponível em: CMC | Network Log-Based SSH Brute-Force Attack Detection Model (techscience.com). Acesso em: 28 maio 2023.

PUTRA, Dewa M. J.; ANANTRA, Nyoman N. Y.; KUSUMA Putu A.; PRATAMA, Putu D. J.; SASKAR, Gede A. J.; Listartha, Made E. **ANALISIS PERBANDINGAN SERANGAN HYDRA, MEDUSA DAN NCRACK PADA PASSWORD ATTACK**. Disponível em: <https://jurnal.uts.ac.id/index.php/JINTEKS/article/view/2192>. Acesso em: 26 mai 2024.

RAHARDHITA, Widyatra S.; NOBUO, Funabiki; MINORU, Kuribayashi; KWENGA, Ismael M.; MANOWARUL, Islam. **A TCP Fairness Control Method for Two-Host Concurrent Communications in Elastic WLAN System Using Raspberry Pi Access-Point**. Disponível em: <https://ieeexplore.ieee.org/document/8726907>. Acesso em: 26 mai 2024.

RAJU A. Nadaf; RUBINA M.; SUJATA, P.; VASUDHA, M. Bonal. **Smart Mirror Using Raspberry Pi for Human Monitoring and Intrusion Detection**. Disponível em: <https://ieeexplore.ieee.org/document/8987294>. Acesso em: 25 mai 2024.

ROHITH, Raj S; ROHITH, R; MINAL, Moharir. SHOBHA, G. SCAPY- **A powerful interactive packet manipulation program**. Disponível em: <https://ieeexplore.ieee.org/document/8903954>. Acesso em: 25 mai 2024.

SADASIVAM, Gokul K; HOTA, Chinttaranjan; ANAND, Bhojan. **Honeynet Data Analysis and Distributed SSH Brute-Force Attacks**. Disponível em: https://link.springer.com/chapter/10.1007/978-981-13-2348-5_9. Acesso em: 22 agosto 2023.

SHIPRA, Bansal; NITIN, Bansal. **Scapy – A python Tool for Security Testing**. Disponível em: <https://www.semanticscholar.org/paper/Scapy%E2%80%93Python-Tool-For-Security-Testing-Bansal-/Bansal/64f877e82b434a05f1633cb5677e8f946feb165d>. Acesso em: 24 mai 2024.

WANJAU, Stephen K.; WAMBUGU, Geoffrey M.; KAMAU, Gabriel N. **SSH-Brute Force Attack Detection Model based on Deep Learning**. Disponível em: <ijcatr10011008.pdf>. Acesso em: 23 maio 2023.