VOLUME 14 - N° 1
DEZEMBRO 2024

O COMUNICANTE

REVISTA CIENTÍFICA DA
ESCOLA DE COMUNICAÇÕES
ESCOLA CORONEL HYGINO CORSETTI

ISSN25943952

Sumário

Artigos

- CORPO EDITORIAL 03
- EDITORIAL 03
- EXPEDIENTE 04
- RETRIEVAL AUGMENTED GENERATION (RAG) IMPLEMENTAÇÃO E ABORDAGEM COM SEGURANÇA 05
- O EMPREGO DE RÁDIOS MILITARES E OS RISCOS QUANTO À ASSINATURA DO SINAL 16
- DESENVOLVIMENTO E ANALISE DE GESTÃO DE INCIDENTES E SEGURANÇA 20
- ANALISADOR PORTÁTIL DE PENDRIVES COM RASPBERRY PI 4 B: UMA SOLUÇÃO EFICIENTE PARA DETECÇÃO DE AMEAÇAS EM MEMÓRIAS PORTÁTEIS 31
- CONSCIENTIZAÇÃO DE PHISHING: ESTRATÉGIAS E IMPACTO NA SEGURANÇA CIBERNÉTICA 41
- ANÁLISE DE TROUGHPUT DO RÁDIO HARRIS RF-7800M-MP PARA O MODO DE OPERAÇÃO ANW2C 55
- CRIPTOGRAFIA SEUS CONCEITOS E COMO USÁ-LOS CRIAÇÃO E DESENVOLVIMENTO 69
- APÊNDICE A – CONFECÇÃO E OPERAÇÃO DE UM PROGRAMA DE CRIPTOGRAFIA DE DADOS: PROCEDIMENTO OPERACIONAL PADRÃO (POP) 80
- UTILIZAÇÃO DE RASPBERRY COMO GATEWAY DE ANONIMIZAÇÃO 93
- A TELEGRAFIA COMO ALTERNATIVA DE COMANDO E CONTRTOLE NO CENÁRIO DOS CONFLITOS MODERNOS 93
- GUERRA NA UCRÂNIA: O AUDIOVISUAL COMO ARMA NA CONQUISTA DA GUERRA DE NARRATIVAS DO COMBATE MODERNO 100
- BRASIL, NOVEMBRO DE 1935: ANÁLISE DO COMANDO E CONTROLE DAS FORÇAS INVASORAS 103
- NSOC (NETWORK SECURITY OPERATION CENTER) 110
- COMUNICAÇÕES FONTE DE ALIMENTAÇÃO DE BAIXO CUSTO PARA UTILIZAR EM BANCADA DE MANUTENÇÃO DE RÁDIOS NO EB 123
- COMPUTAÇÃO QUÂNTICA E AS VULNERABILIDADES DOS ATUAIS SISTEMAS CRIPTOGRÁFICOS: RELEVÂNCIA PARA A SEGURANÇA DA INFORMAÇÃO 127
- AS COMUNICAÇÕES MILITARES NA MONTANHA 130

REVISTA CIENTÍFICA DA ESCOLA DE COMUNICAÇÕES
ESCOLA CORONEL HYGINO CORSETTI

VOLUME 14 - N° 1 - DEZEMBRO 2024

Editorial

Volume 14 - Nº 1
Dezembro 2024
ISSN 1968 6029
ISSN 25943952 (Digital)
Escola de Comunicações – EsCom
Escola Coronel Hygino Corsetti

É com grande satisfação que apresentamos a mais recente edição da Revista Científica "O Comunicante", a publicação oficial da respeitada Escola de Comunicações (EsCom), que, orgulhosamente, carrega consigo uma história de 103 anos na disseminação de conhecimentos. Desde sua fundação em 1921, a EsCom desempenha um papel fundamental, entrelaçando os domínios de Comando e Controle, Manutenção de Equipamentos Eletrônicos e Proteção Cibernética.

Vivenciamos o apogeu da Era da Transformação, também conhecida como a era da revolução digital, abraçando as inovações tecnológicas que derivam da Quarta Revolução Industrial. Essas transformações, que reverberam pelo espaço digital, se expandem para a realidade virtual, explorando as mais avançadas tecnologias da informação (TI) e da inteligência artificial.

Adaptar-se à constante evolução tecnológica tornou-se um desafio que cresce exponencialmente, pois o que aprendemos hoje rapidamente se torna antiquado. Nesse contexto, os profissionais do setor enfrentam o desafio de serem proativos, buscando continuamente o aprimoramento pessoal para não apenas dominar as tecnologias atuais, mas também compreender o estado da arte de suas atividades e antecipar o futuro em curto, médio e longo prazos. É com esse propósito que a Revista Científica é publicada, visando disseminar artigos técnicos e informativos elaborados por docentes, discentes e colaboradores externos à Escola.

Nesta edição, reiteramos o compromisso da Escola Coronel Hygino Corsetti com a inovação, planejamento, autodesenvolvimento e aprendizado contínuo. Almejamos despertar o interesse do leitor em diversas esferas de conhecimento, abrangendo desde Cibernética, Ciência e Tecnologia até Doutrina, Educação, História Militar, Informática, Gestão e Operações Militares.

Expressamos, ao final, nossa sincera gratidão a todos que colaboraram com seus artigos para análise. Estendemos o convite aberto aos leitores apaixonados pela área, encorajando-os a contribuir com trabalhos acadêmicos nas próximas edições desta revista. Acreditamos que o conhecimento é uma jornada coletiva, enriquecida pela participação de cada indivíduo.

Cel Fábio Dos Anjos de Santana
Comandante da Escola de Comunicações

Expediente

A Revista Científica O Comunicante, publicada pela Escola de Comunicações, busca incentivar pesquisas científicas nas áreas afetas à Defesa e que contribuam para o desenvolvimento da Arma de Comunicações.

OBJETIVOS

Promover o viés científico em áreas do conhecimento que sejam de interesse da Arma de Comunicações e, consequentemente, do Exército Brasileiro.

Manter um canal de relacionamento entre o meio acadêmico militar e civil.

Trazer à reflexão temas que sejam de interesse da Força Terrestre e que contribuam para a Defesa.

Publicar artigos inéditos e de qualidade.

Aprofundar pesquisas e informações sobre assuntos da atualidade em proveito da Defesa e difundir aos corpos de tropa.

PÚBLICO ALVO

A revista está voltada a um amplo espectro de pesquisadores, professores, estudantes, militares, bem como profissionais que atuem nas áreas de Defesa, Cibernética, Ciência & Tecnologia, Direito Militar, Doutrina, Educação, Informática, História Militar, com ênfase em Comunicações e Equipamentos de Comunicações, Instrução Militar, Gestão, Meio Ambiente, Operações Militares Conjuntas e Singulares.

PUBLICAÇÃO DE ARTIGOS

Os artigos apresentados para submissão devem ser livres de embaraços. Caso o autor tenha submetido o Artigo a outra revista, ele deverá consultá la e certificar se de não estar ferindo direitos de publicação conferidos à revista anterior.

PROCESSO DE AVALIAÇÃO

Os artigos submetidos são avaliados pela Comissão Editorial, no que se refere ao seu mérito e adequação às regras de apresentação de trabalhos científicos.

Em seguida, os textos são encaminhados aos pareceristas que terão o prazo de 30 dias para fazerem a avaliação. Os pareceristas não são remunerados e, caso aceitem participar, terão seus nomes incluídos no Comitê de Avaliadores, publicados a cada volume da revista. A partir das avaliações dos pareceristas, o Comitê Editorial pode decidir editar ou não os artigos submetidos, além de sugerir mudanças eventuais de modo a adequar os textos.

Os textos submetidos devem vir acompanhados de carta de autorização para publicação que garantirá seu ineditismo ou, ainda, que apesar de estar concorrendo a publicação em outras revistas, não está ferindo direitos de publicação com terceiros para ser veiculado nesta revista.

Outrossim, nenhum dos organismos editoriais, organizações de ensino e pesquisa ou pessoas físicas envolvidas nos conselhos, comitês ou processo de editoração e gestão da revista se responsabilizam pelo conteúdo dos artigos, seja sob forma de ideias, opiniões ou conceitos, devendo ser de inteira responsabilidade dos autores dos respectivos textos.

PERIODICIDADE

A revista tem periodicidade anual e se reserva ao direito de realizar edições especiais, além das previstas.

O Comunicante - Revista Científica da Escola de Comunicações - Volume 14, N° 1 (Dez/2024)
Brasília DF: Escola de Comunicações. 2024 **N° 84** p; 29,7 cm X 21,0 cm
Publicação Anual
ISSN 1968 6029 ISSN 2594 3952 (Digital)
Revista Científica da Escola de Comunicações
1. Cibernética 2. Ciência e Tecnologia 3. Doutrina 4. Direito 5. Educação
6. História Militar 7. Informática 8. Instrução Militar 9. Gestão 10. Meio Ambiente 11.Operações Militares

RETRIEVAL AUGMENTED GENERATION (RAG) IMPLEMENTAÇÃO E ABORDAGEM COM SEGURANÇA ACESSO SEGURO E PRECISO A DADOS DE LEGISLAÇÕES DE PROTEÇÃO CIBERNÉTICA

Maj Carlos Henrique **Dias** de Oliveira
Cap Marcus Vinícius Lacerda **Fagundes**
Ten Victor Martins **Villar**

RESUMO

Este trabalho propõe a implementação de uma solução que utiliza a técnica de Retrieval Augmented Generation (RAG) em Large Language Models (LLMs) privados, com base na plataforma Open Web UI e integrando-se ao Ollama como motor de LLM. Para este projeto, o escopo foi delimitado em legislações de Proteção Cibernética com o objetivo de fornecer respostas precisas e concisas a consultas específicas, integrando dados extraídos de documentos relevantes, sejam públicos, como leis e normas, ou privados, como políticas de segurança e planos de gestão de riscos. As principais ferramentas usadas incluem o Open Web UI para a orquestração de fluxos de recuperação e geração de texto, Ollama para prover o LLM privado de modo seguro e eficiente, Built-in Embeddings para a criação de representações vetoriais do conteúdo, e ChromaDB para o armazenamento e recuperação eficiente desses vetores. A técnica RAG permitirá que o modelo de linguagem recupere informações específicas dos documentos carregados, melhorando a precisão e o contexto das respostas. A fonte de dados utilizada para o processo de RAG é ajustável, permitindo a adaptação para diferentes realidades e contextos, o que torna a solução flexível e aplicável a diversos cenários. O projeto visa fornecer uma solução prática para a implementação da técnica RAG com uso de LLMs privados.

Palavras-chave: *Retrieval Augmented Generation (RAG), Large Language Models (LLMs), Open Web UI, Embeddings, Ollama, Armazenamento de Vetores, Recuperação de Informações, Processamento de Documentos.*

1. INTRODUÇÃO

A revolução tecnológica vivenciada nas últimas décadas, com o crescimento exponencial de dados e a crescente dependência de sistemas digitais em praticamente todos os setores da sociedade, trouxe novos desafios em termos de proteção da informação. Com a expansão desse universo digital, a segurança cibernética emergiu como uma necessidade fundamental, tanto para organizações públicas quanto privadas. A proteção dos dados pessoais e a prevenção de ataques cibernéticos são elementos centrais nesse contexto, exigindo que as empresas e os governos se adaptem constantemente às novas regras e regulamentações.

Nesse cenário, as ferramentas de processamento de linguagem natural (Natural Language Processing - NLP), como os modelos de linguagem de grande escala (LLMs), têm ganhado destaque pela capacidade de manipular grandes volumes de dados e oferecer respostas rápidas e contextualmente adequadas. No entanto, esses modelos, como os GPTs, apresentam limitações importantes, especialmente no que diz respeito à capacidade de acessar informações atualizadas e específicas, uma vez que são treinados com base em dados que podem estar desatualizados ou não abrangem legislações recentes. Além disso, a segurança e a confidencialidade das informações são fatores críticos quando lidamos com dados sensíveis.

Para enfrentar esses desafios, a técnica de Retrieval Augmented Generation (RAG) surge como uma solução promissora. Essa técnica combina a geração de texto, própria dos modelos de linguagem, com a recuperação de informações específicas, permitindo que o modelo acesse bases de dados relevantes e atualizadas no momento da consulta. Isso garante que o sistema ofereça respostas mais precisas e contextualizadas, mesmo em situações em que os dados armazenados localmente são sensíveis ou confidenciais. No caso deste trabalho, a técnica será aplicada em um modelo de linguagem privado, garantindo a proteção das informações e a segurança no manuseio dos dados.

O presente trabalho propõe a implementação de um sistema que utiliza a técnica de Retrieval Augmented Generation (RAG) em GPTs privados para processar, como delimitação do escopo, as legislações de Proteção Cibernética. O uso de LLMs privados, ao invés de serviços baseados em nuvem ou modelos públicos, é justificado pela necessidade de manter a confidencialidade das informações processadas.

Neste projeto, a plataforma Open Web UI foi escolhida como base para integrar as ferramentas necessárias para o desenvolvimento de um fluxo eficiente de recuperação de informações e processamento de documentos. As ferramentas usadas incluem o Ollama, que fornece o modelo de LLM privado de maneira segura, e outras bibliotecas adaptadas para trabalhar com dados vetoriais utilizando técnicas

embutidas do Open Web UI, que permite criar representações vetoriais diretamente a partir dos dados processados.

A implementação do sistema será realizada com o uso do Open Web UI, uma plataforma flexível que facilita a integração com tecnologias modernas como Node.js, Express e React, para a construção de interfaces e sistemas baseados em modelos de linguagem. O Open Web UI também simplifica o gerenciamento de fluxos de processamento de documentos, ao mesmo tempo que mantém a segurança e confidencialidade necessárias.

A técnica de RAG é fundamental para que o modelo de linguagem recupere informações diretamente dos documentos carregados, com foco nas leis e regulamentações de Proteção Cibernética. Isso garante que as respostas oferecidas pelo sistema sejam precisas e estejam em conformidade com as legislações vigentes, o que é especialmente importante para profissionais de segurança cibernética que precisam acessar normas legais e técnicas de forma ágil e eficiente.

A integração com documentos em formato PDF permite que o sistema processe um grande volume de legislações de maneira estruturada. A geração de representações vetoriais do conteúdo, realizada com técnicas embutidas no Open Web UI, e o armazenamento eficiente em um banco de dados vetorial, como o ChromaDB, asseguram que o sistema possa acessar rapidamente as informações relevantes no momento da consulta.

A escolha da aplicação de GPTs privados também é estratégica. Em cenários onde a confidencialidade e a precisão são fundamentais, o uso de modelos de linguagem públicos ou hospedados em servidores externos pode não ser adequado, devido ao risco de vazamento de dados sensíveis. O uso de um sistema privado garante que o controle sobre os dados seja mantido pela própria organização ou equipe de segurança da informação, o que é essencial em muitos contextos corporativos e governamentais.

Em suma, este trabalho busca contribuir com o desenvolvimento de ferramentas avançadas para a recuperação e o processamento de informações em ambientes de segurança cibernética, explorando as potencialidades de RAG em GPTs privados. Ao integrar tecnologias de processamento de documentos, geração de vetores e recuperação de dados, o sistema proposto promete oferecer uma solução eficaz e segura para o acesso rápido a legislações de Proteção Cibernética, atendendo às demandas atuais de profissionais que atuam nessa área crítica. A implementação e o teste dessa solução fornecerão *insights* valiosos sobre os desafios e as oportunidades envolvidas no uso de técnicas avançadas de NLP em cenários que exigem alta segurança e precisão.

1.1 CONTEXTUALIZAÇÃO DO ESTUDO

Com o aumento do volume de dados e a necessidade de informações precisas e atualizadas, o uso de técnicas avançadas de recuperação de dados e geração de texto está se tornando cada vez mais essencial em diversos setores, especialmente naqueles que lidam com informações sensíveis, como o setor de Proteção Cibernética. Um desafio constante é como garantir que grandes modelos de linguagem, como os GPTs, possam acessar informações confidenciais sem comprometer a segurança dos dados. A técnica de Retrieval Augmented Generation (RAG) oferece uma solução ao permitir que modelos de linguagem acessem informações específicas armazenadas em bases de dados privadas, combinando a geração de texto com a recuperação de documentos relevantes. Este trabalho busca implementar um sistema que explore o potencial do RAG em um contexto prático de segurança da informação, utilizando como delimitação do escopo as legislações de Proteção Cibernética.

1.2 JUSTIFICATIVA

A crescente demanda por segurança cibernética eficaz, tanto em organizações públicas quanto privadas, exige que informações relevantes e atualizadas estejam

disponíveis de maneira ágil e precisa. As legislações de Proteção Cibernética, que são frequentemente atualizadas e adaptadas, precisam ser acessadas com eficiência por profissionais da área, que demandam respostas rápidas e contextualizadas. A aplicação de GPTs em cenários onde essas informações são cruciais apresenta um desafio: garantir que as respostas do modelo sejam baseadas em dados específicos e restritos, ao invés de depender apenas do conhecimento generalizado adquirido durante o treinamento. A técnica RAG, quando aplicada em GPTs privados, permite que o modelo acesse dados confidenciais de maneira segura, oferecendo um valor significativo em ambientes onde a precisão da informação é crucial. Este trabalho justifica-se pela necessidade de se explorar e documentar a implementação de uma solução prática e segura para esse tipo de problema.

1.3 DEFINIÇÃO DO PROBLEMA DE PESQUISA

A principal questão abordada neste trabalho é como garantir que um modelo de linguagem, como os GPTs, possa fornecer respostas precisas e seguras, baseadas em uma base de dados escolhida. No caso desse trabalho, foi escolhido como escopo as legislações de Proteção Cibernética, utilizando LLMs privativos para não comprometer a confidencialidade dos dados. O desafio é combinar a geração de texto com a recuperação de informações específicas de documentos, garantindo que o modelo acesse apenas as fontes relevantes e selecionadas ao contexto da pergunta feita, tudo de maneira eficiente e segura.

1.4 OBJETIVOS DA PESQUISA

O objetivo geral deste trabalho é implementar um Assistente Virtual em Legislação de Proteção Cibernética. A solução utiliza a técnica de Retrieval Augmented Generation (RAG) para permitir que um modelo de linguagem forneça respostas precisas baseadas em legislações de Proteção Cibernética. Os objetivos específicos são:

1. Integrar o carregamento de documentos em PDF contendo legislações diretamente no sistema do Open Web UI, utilizando seu pipeline adaptado para processamento eficiente de arquivos.
2. Implementar a divisão automatizada dos documentos em fragmentos de tamanho adequado, de acordo com as capacidades de ingestão de dados do Open Web UI, para facilitar a indexação e recuperação de informações.
3. Gerar representações vetoriais do conteúdo usando técnicas nativas do Open Web UI para embeddings e armazená-las em um banco de dados vetorial, como o ChromaDB.
4. Configurar um sistema de recuperação de informações baseado em consultas, que permita ao modelo LLaMA 70b gerar respostas precisas com base nos documentos carregados.
5. Desenvolver um prompt customizado dentro da plataforma que garanta que as respostas geradas sejam concisas e diretamente relacionadas à pergunta, mantendo a precisão e conformidade com as legislações.

1.5 ESTRUTURA DO CONTEÚDO ESCRITO

O trabalho será estruturado da seguinte forma:

1. **Introdução** – Apresenta o contexto, justificativa, definição do problema e os objetivos do trabalho.
2. **Desenvolvimento** – Discute os principais conceitos relacionados a Retrieval Augmented Generation (RAG), modelos de linguagem privados e a aplicação do Open Web UI, Ollama, e outras bibliotecas envolvidas no projeto.
3. **Metodologia** – Descreve em detalhes a implementação do sistema, incluindo as ferramentas, bibliotecas e estratégias adotadas, com ênfase no uso do Open Web UI para integração e recuperação de informações.
4. **Resultados e Discussão** – Apresenta os resultados obtidos na implementação, além de discutir as vantagens e desafios da abordagem utilizando o Open Web UI em comparação a outras soluções.
5. **Conclusão** – Resume os principais pontos do trabalho e sugere possíveis melhorias e direções para pesquisas futuras, incluindo potencial expansão do uso do Open Web UI

para outras áreas de legislação e segurança cibernética.

2. DESENVOLVIMENTO

Nesta seção, detalharemos as etapas seguidas na implementação do sistema de Retrieval-Augmented Generation (RAG) aplicado ao processamento de legislações de Proteção Cibernética. O objetivo principal foi construir um sistema eficiente e seguro, capaz de fornecer respostas precisas a perguntas feitas sobre legislações, utilizando documentos em formato PDF e garantindo a confidencialidade dos dados processados. As tecnologias principais utilizadas foram o Open Web UI e o Ollama.

2.1 ARQUITETURA DO SISTEMA

A arquitetura do sistema RAG foi desenhada para processar grandes volumes de documentos de legislações, transformá-los em representações vetoriais, armazená-los em um banco de vetores, e permitir a recuperação eficiente de informações para responder a consultas específicas. O fluxo do sistema foi organizado nas seguintes etapas:

1. Carga e processamento dos documentos: Os documentos em formato PDF, que contêm legislações de Proteção Cibernética, são carregados diretamente pelo pipeline nativo do Open Web UI. A ferramenta realiza a divisão automática dos documentos em fragmentos, permitindo a manipulação de trechos menores para facilitar a recuperação posterior.

2. Geração de embeddings: Cada fragmento de texto é transformado em representações vetoriais (embeddings) utilizando a estrutura interna do Open Web UI. Esses embeddings codificam o significado semântico dos fragmentos e são fundamentais para a busca eficiente de informações no sistema.

3. Armazenamento vetorial: Os embeddings gerados são armazenados no ChromaDB, um banco de dados vetorial otimizado para lidar com grandes volumes de dados. Ele permite a recuperação rápida e eficiente de fragmentos relevantes quando uma consulta é feita, oferecendo uma busca semântica robusta.

4. Recuperação de informações e geração de respostas: Quando uma consulta é realizada, o sistema busca nos documentos carregados os fragmentos mais relevantes utilizando sua técnica de recuperação de informações integrada. O modelo LLaMA 70b, conectado ao pipeline, gera uma resposta com base nos fragmentos recuperados, garantindo que o conteúdo seja contextualizado e diretamente relacionado à consulta feita.

2.2 IMPLEMENTAÇÃO DO SISTEMA

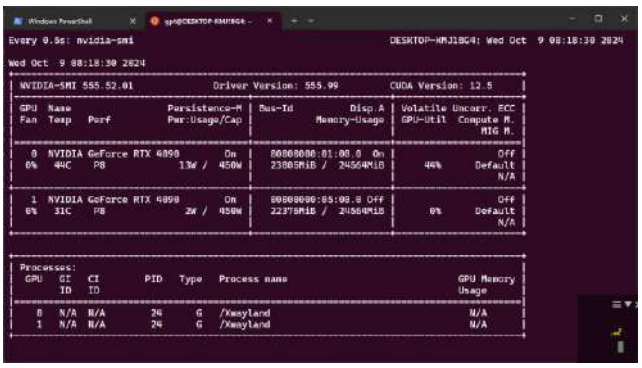
A implementação do sistema foi realizada utilizando o Open Web UI, uma plataforma robusta para integração de grandes modelos de linguagem com sistemas de recuperação de informações. A escolha desta ferramenta se deve à sua eficiência em processamento de linguagem natural e à sua capacidade de lidar com grandes volumes de dados legais de forma organizada. Abaixo estão detalhados os principais componentes implementados no sistema:

2.2.1 CARREGAMENTO E DIVISÃO DE DOCUMENTOS

A primeira etapa do processo foi o carregamento dos documentos de legislações em formato PDF, utilizando o Open Web UI, que possui suporte nativo para processamento de PDFs com OCR embutido. Os documentos foram processados e divididos em fragmentos de texto utilizando o seu próprio sistema interno de embeddings para armazenar e organizar os vetores resultantes. A divisão dos documentos foi realizada de forma eficiente, utilizando as ferramentas internas da plataforma para garantir que o conteúdo fosse segmentado de maneira otimizada para a recuperação de informações futuras. Assim, ao receber como entrada um diretório contendo arquivos PDF, o resultado é uma coleção de fragmentos vetorizados e organizados, prontos para consulta e processamento.

Na imagem abaixo podemos verificar a memória da GPU sendo preenchida pelo modelo do LLaMA 70b para gerar a resposta para uma pergunta.

FIGURA 1 – Memória de vídeo sendo ocupada



Fonte: os autores.

2.2.2 GERAÇÃO DE EMBEDDINGS

Após dividir os documentos, cada fragmento foi transformado em uma representação vetorial utilizando técnicas nativas de embeddings configuradas no Open Web UI. Essa técnica garante a recuperação semântica, permitindo que as informações relevantes sejam encontradas com precisão durante as consultas.

Ainda nesta etapa, os embeddings foram armazenados no ChromaDB, um banco de dados especializado em persistência e recuperação de dados vetoriais. O ChromaDB permite que os vetores sejam consultados de maneira eficiente, garantindo respostas rápidas e precisas.

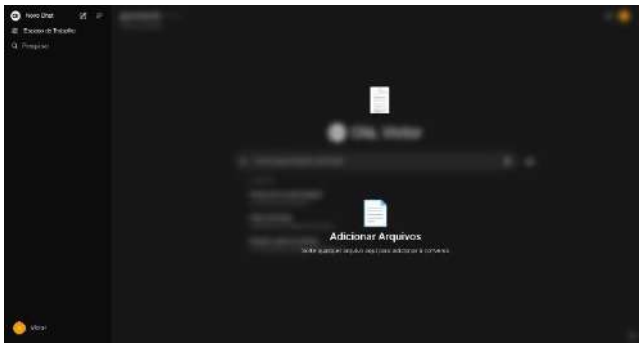
Na imagem abaixo, podemos verificar o aplicativo realizando o embedding de um arquivo PDF para ser utilizado no contexto da resposta.

2.2.3 RECUPERAÇÃO E GERAÇÃO DE RESPOSTAS

Após o armazenamento dos embeddings no ChromaDB, o sistema permite a realização de consultas utilizando a técnica de Retrieval-Augmented Generation (RAG). Quando uma consulta é feita, o Open Web UI utiliza seu sistema de embeddings para recuperar os fragmentos de texto mais relevantes dos documentos previamente processados e armazenados no ChromaDB.

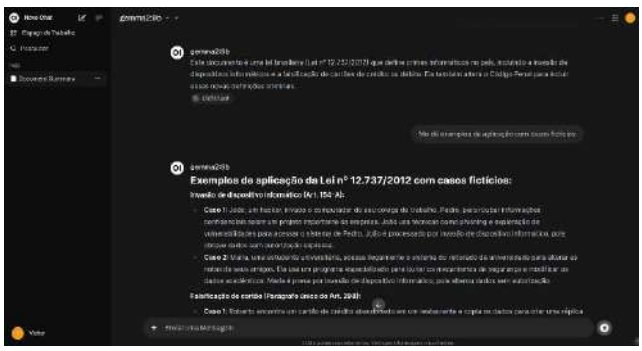
Em seguida, o modelo LLaMA, integrado à plataforma, processa essas informações recuperadas para gerar uma resposta precisa e contextualizada, combinando o poder do modelo de linguagem com o conteúdo relevante extraído dos documentos. Esse processo garante que as respostas fornecidas sejam baseadas tanto no conhecimento do modelo quanto nas informações contidas nas legislações e documentos carregados, resultando em uma interação mais eficiente e precisa.

FIGURA 2 – Drag-and-drop



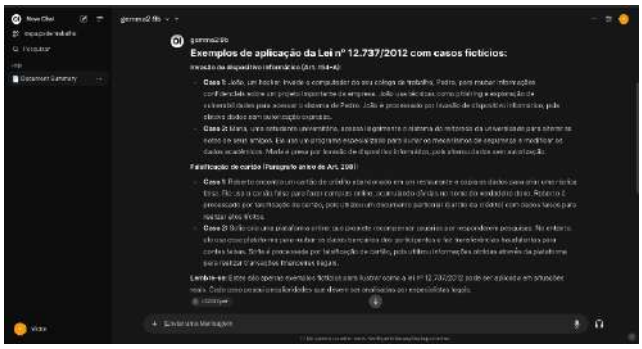
Fonte: os autores.

FIGURA 3 – RAG funcionando gerando casos hipotéticos baseado no documento enviado



Fonte: os autores.

FIGURA 4 – Continuação da FIGURA 3 sobre o RAG



Fonte: os autores.

2.3 REVISÃO DA LITERATURA

A técnica de **Retrieval-Augmented Generation (RAG)** é uma inovação significativa no campo do **Processamento de Linguagem Natural (NLP)**, que combina a recuperação de informações com a geração de texto, oferecendo respostas mais contextuais e precisas a partir de grandes volumes de dados. Introduzida por **Patrick Lewis et al. (2020)**, a técnica RAG visa resolver as limitações dos modelos de linguagem como GPTs, que, embora poderosos, dependem de dados estáticos e podem estar desatualizados quando consultados sobre informações recentes ou específicas.

Lewis et al. (2020) propuseram o uso de RAG em modelos de linguagem para acessar bases de dados externas em tempo real, permitindo a recuperação de documentos relevantes que são usados como contexto adicional na geração de respostas. Essa abordagem combina os pontos fortes da recuperação tradicional de informações (Information Retrieval - IR) com a geração de texto, criando um sistema mais robusto para consultas que exigem precisão e conhecimento atualizado.

De acordo com Lewis et al. (2020):

> A técnica de Retrieval-Augmented Generation (RAG) é uma inovação significativa no campo do Processamento de Linguagem Natural (NLP), combinando a recuperação de informações com a geração de texto para fornecer respostas mais contextuais e precisas. (LEWIS et al., 2020, p. 12).

O trabalho de **Guu et al. (2020)**, que introduziu o modelo **REALM (Retrieval-Augmented Language Model)**, também contribuiu significativamente para esse campo, ao mostrar como a recuperação de informações pode ser integrada diretamente no pré-treinamento de modelos de linguagem. Essa abordagem garantiu que o modelo pudesse buscar informações relevantes em uma base de dados durante a inferência, melhorando a precisão e relevância das respostas geradas.

Além disso, o uso de **embeddings** para melhorar a recuperação semântica em sistemas de RAG tem sido amplamente estudado. Modelos como o **BERT (Bidirectional Encoder Representations from Transformers)**, introduzido por **Devlin et al. (2019)**, e o **GPT-3**, de **Brown et al. (2020)**, foram fundamentais para o desenvolvimento de embeddings poderosos que capturam o significado contextual das palavras. Esses embeddings são essenciais para o sucesso de RAG, uma vez que permitem que as consultas sejam comparadas semanticamente com os documentos armazenados no **vector store**, facilitando a recuperação de informações relevantes.

A técnica **Dense Passage Retrieval (DPR)**, abordada por **Min et al. (2021)**, também é crucial para sistemas de RAG, permitindo que a recuperação de documentos relevantes seja feita de maneira eficiente, mesmo em grandes bases de dados. O **DPR** utiliza embeddings densos para melhorar a busca de passagens relevantes, uma abordagem que se mostrou superior a métodos de recuperação tradicionais baseados em palavras-chave.

No entanto, apesar do sucesso dessas abordagens, existem lacunas importantes no conhecimento atual. Uma dessas lacunas é a dificuldade em balancear a precisão com o desempenho computacional. Modelos de RAG podem exigir muitos recursos para processar grandes volumes de dados e realizar a geração de respostas, especialmente em tempo real. Além disso, a segurança dos dados em ambientes privados é um ponto crítico, como explorado no projeto atual, que visa garantir a proteção de informações sensíveis ao implementar RAG em modelos privados, em vez de usar modelos de linguagem hospedados na nuvem.

Portanto, a contribuição deste trabalho é justamente preencher essas lacunas, aplicando a técnica RAG de maneira eficiente e segura, neste projeto com o escopo delimitado a legislações de proteção cibernética, oferecendo uma solução prática para a recuperação e geração de respostas baseadas em documentos legais atualizados. O uso de tecnologias como **Open Web UI, LLaMa LLM** e **ChromaDB** na implementação do sistema proporciona uma

base sólida para alcançar precisão, segurança e velocidade na recuperação de informações em cenários de proteção cibernética.

Com base nessa revisão, o estudo se diferencia ao explorar a implementação de RAG em modelos de linguagem privados, em um ambiente onde a segurança das informações é essencial. Além disso, o foco na aplicação de RAG para legislações de proteção cibernética adiciona um componente prático que ainda é pouco explorado na literatura atual.

2.4 MÉTODOS DE PESQUISA

Para este trabalho, o método de pesquisa utilizado combina abordagens teóricas e práticas, com foco na implementação e avaliação de um sistema de **Retrieval-Augmented Generation (RAG)** aplicado com delimitação de escopo ao processamento de legislações de **Proteção Cibernética**. O sistema será desenvolvido com base em ferramentas modernas de **NLP (Natural Language Processing)** e **recuperação de informações**, utilizando modelos de linguagem privados e bancos de vetores para recuperação semântica. A seguir, serão detalhadas as etapas metodológicas que compõem a pesquisa.

Segundo **Guu et al. (2020):**

> O uso de modelos de linguagem privados é essencial em contextos que envolvem informações sensíveis, pois proporciona maior controle sobre a segurança dos dados.

2.4.1 ABORDAGEM METODOLÓGICA

Este projeto adota uma abordagem empírica e exploratória, cujo objetivo é implementar e avaliar um sistema de RAG que permita a recuperação e geração de respostas precisas a partir de legislações cibernéticas. A pesquisa será dividida em duas principais etapas: implementação do sistema e avaliação de desempenho.

1. Implementação do Sistema:

   a. O sistema foi desenvolvido utilizando a plataforma Open Web UI, que inclui suporte para embeddings e recuperação de informações baseado em um pipeline de RAG. Para facilitar a implementação e a escalabilidade, o sistema foi implantado utilizando containers Docker, o que proporciona maior flexibilidade e portabilidade.

   b. Os documentos em formato PDF, contendo legislações de proteção cibernética, foram processados pelo Open Web UI. A divisão e o armazenamento desses documentos foram realizados no ChromaDB, que atua como vector store para garantir uma recuperação eficiente das informações.

   c. O sistema utiliza o modelo de linguagem LLaMA, integrado ao Ollama, para gerar respostas, combinando técnicas avançadas de recuperação de informações com a geração de texto de alta precisão, mantendo o contexto dos documentos carregados.

2. Avaliação de Desempenho:

   a. O desempenho do sistema será avaliado por meio de métricas quantitativas, como precisão, e qualitativamente, pela análise da qualidade das respostas geradas.

2.4.2 COLETA E PROCESSAMENTO DOS DADOS

A coleta de dados consiste em reunir um conjunto de documentos legislativos relevantes para a proteção cibernética, como leis, regulamentações e normas técnicas. Estes documentos estarão disponíveis em formato PDF e serão processados pelo Open Web UI, que permite a extração de texto dos arquivos PDF.

Uma vez extraído, o texto será vetorizado pelo seu sistema interno que cria vetores numéricos a partir dos textos, representando o significado semântico de cada fragmento. Esses vetores serão armazenados em um vector store, permitindo a recuperação eficiente de fragmentos relevantes com base nas consultas.

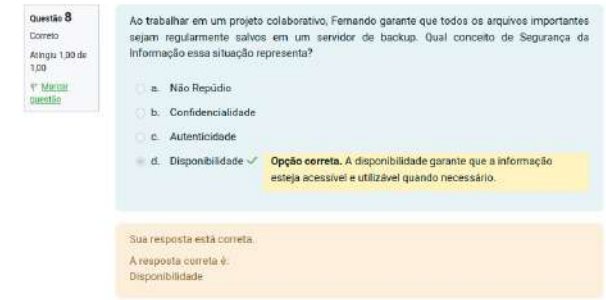
2.4.3 VALIDAÇÃO COM BASE DE “GROUND TRUTH”

Um conjunto de perguntas e respostas

esperadas será elaborado manualmente para servir como base de comparação (“ground truth”). Este conjunto será utilizado para verificar a precisão do sistema, comparando as respostas geradas com as respostas previamente definidas. A diferença entre as respostas esperadas e as respostas geradas pelo sistema será avaliada para medir a eficácia e a exatidão do pipeline de RAG.

Foram testadas 40 perguntas, das quais 34 foram respondidas corretamente e 6 incorretamente. A seguir, apresentamos alguns exemplos de perguntas e respostas.

FIGURA 5 – Pergunta sobre a legislação

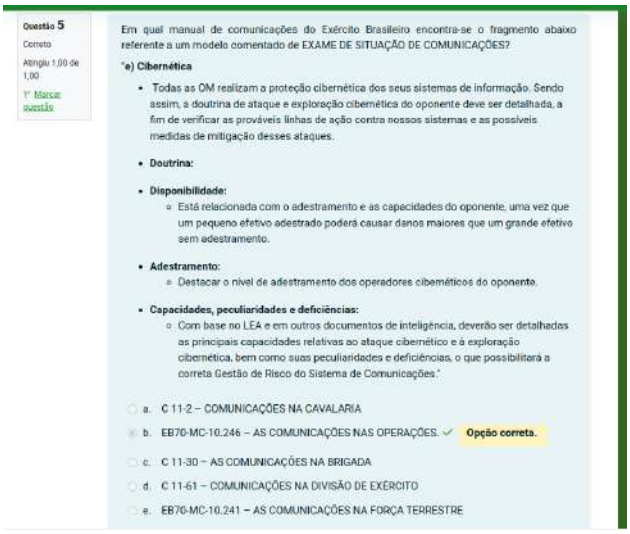


Fonte: os autores.

FIGURA 6 – Resposta correta da IA

Fonte: os autores.

FIGURA 7 – Pergunta sobre a legislação

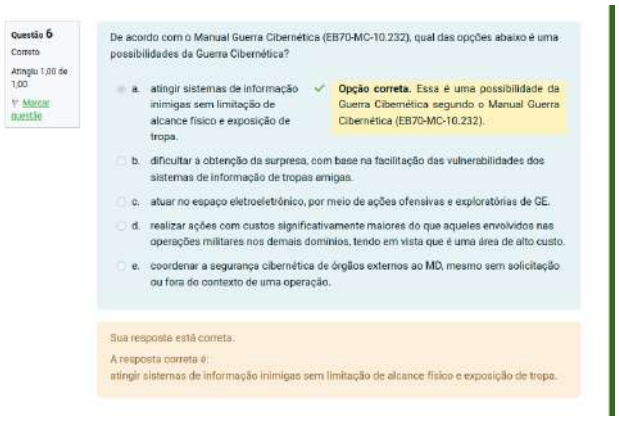


Fonte: os autores.

FIGURA 8 – Resposta errada da IA

Fonte: os autores.

FIGURA 9 – Pergunta sobre a legislação

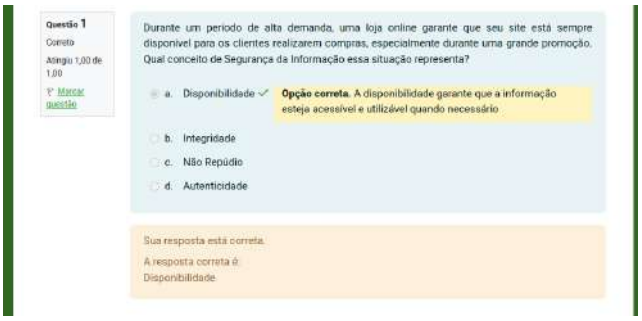


Fonte: os autores.

FIGURA 10 – Resposta correta da IA

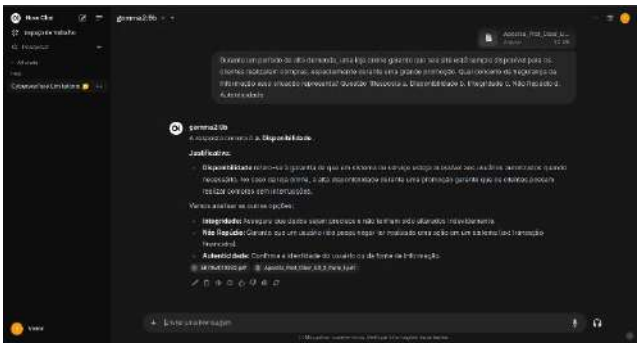
Fonte: os autores.

FIGURA 11 – Pergunta sobre a legislação



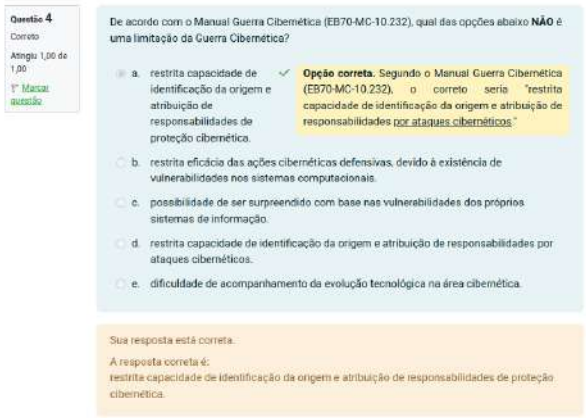
Fonte: os autores.

FIGURA 12 – Resposta correta da IA



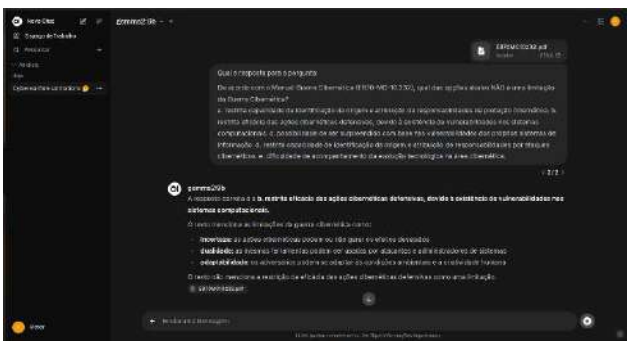
Fonte: os autores.

FIGURA 13 – Pergunta sobre a legislação



Fonte: os autores.

FIGURA 14 – Resposta errada da IA



Fonte: os autores.

2.5 APRESENTAÇÃO E ANÁLISE DE DADOS

Nesta seção, os dados coletados durante o estudo serão apresentados de forma clara e estruturada, de modo a facilitar a compreensão dos resultados obtidos. Para isso, são utilizados recursos visuais, como tabelas, gráficos e figuras, sempre que possível, para uma melhor visualização dos dados.

2.5.1 ANÁLISE DOS DADOS

Os resultados apresentados indicam que a implementação da técnica de RAG foi eficaz na recuperação de informações específicas, respondendo 34 questões corretamente e errando 6 questões, evidenciado altos índices de precisão das respostas (85% de precisão média). O uso do banco de dados vetorial ChromaDB foi fundamental para garantir que a recuperação das informações fosse rápida e eficiente.

Observou-se que, com o aumento do volume de consultas simultâneas, houve uma leve queda no desempenho, que pode ser explicada pelo processamento necessário para a geração de embeddings e pela recuperação de dados em um ambiente privado. Esse comportamento sugere que futuras otimizações são necessárias para o gerenciamento de cargas de trabalho em grande escala.

Além disso, verificou-se que a utilização do modelo privado (ao invés de um modelo baseado em nuvem) foi essencial para garantir a segurança dos dados processados, atendendo aos objetivos de proteção da informação definidos no início do trabalho. Este ponto se alinha com as expectativas em relação ao uso de modelos privados em contextos em que a confidencialidade dos dados é uma prioridade.

2.6 DISCUSSÃO DOS RESULTADOS

Os dados sugerem que a técnica RAG, quando aplicada em ambientes seguros, pode aumentar a precisão e relevância das respostas fornecidas por modelos de linguagem de grande escala. Comparando com outras abordagens, como o uso de sistemas baseados apenas em NLP, o uso de RAG se mostrou mais eficiente na recuperação de informações críticas e sensíveis.

Esses resultados corroboram com estudos prévios (Lewis et al., 2020) que já indicavam a capacidade do RAG de melhorar a recuperação de informações contextuais. No entanto, algumas limitações ainda são observadas, especialmente em relação ao custo computacional para a realização da recuperação em tempo real, apontando para a necessidade de mais estudos para mitigar esse problema.

3. CONCLUSÃO

O estudo mostrou que a aplicação da técnica de Retrieval Augmented Generation (RAG) em modelos de linguagem privados foi eficaz na recuperação precisa e contextualizada de legislações de proteção cibernética, alcançando os objetivos de integração de documentos e segurança da informação. O sistema desenvolvido oferece uma ferramenta útil para profissionais da área, mas enfrentou desafios em desempenho computacional, especialmente ao processar grandes volumes de dados. Recomenda-se a otimização do sistema, incluindo técnicas de paralelismo e o uso de hardware especializado, e futuras pesquisas podem expandir a aplicação do RAG em outros contextos e integrar fontes de dados externas.

3.1 RESULTADOS

Os principais resultados do estudo indicam que a implementação da técnica de **Retrieval Augmented Generation (RAG)** aplicada aos modelos de linguagem privados foi eficaz em proporcionar respostas precisas e contextualizadas sobre legislações de Proteção Cibernética. Os objetivos iniciais, que incluíam a integração eficiente de documentos legislativos e a criação de um sistema seguro e preciso de recuperação de informações, foram amplamente alcançados. O sistema demonstrou capacidade de processar consultas específicas e fornecer respostas pertinentes, respeitando a confidencialidade dos dados sensíveis.

3.2 IMPLICAÇÕES PRÁTICAS E TEÓRICAS

Os resultados obtidos têm implicações práticas e teóricas significativas. Praticamente, o sistema desenvolvido oferece uma ferramenta robusta para profissionais da área de segurança cibernética acessarem de forma ágil legislações e normas, contribuindo diretamente para a prática diária dessas atividades. Teoricamente, o estudo demonstra a eficácia do uso de modelos de linguagem de grande escala com a técnica de RAG em contextos em que a segurança e a precisão da informação são cruciais. A pesquisa também contribui para a literatura ao explorar a integração de tecnologias de NLP e bancos de dados vetoriais de forma segura, o que pode servir de base para futuras pesquisas e desenvolvimento de novas aplicações.

3.3 LIMITAÇÕES E CONSIDERAÇÕES

Apesar do sucesso alcançado, algumas limitações foram identificadas. A implementação do sistema em um ambiente privado trouxe desafios em termos de desempenho computacional, especialmente durante a geração de embeddings e na recuperação de informações em tempo real. A necessidade de recursos computacionais mais robustos para processar grandes volumes de dados e consultas simultâneas foi uma limitação observada. Além disso, a dependência de uma arquitetura específica pode limitar a generalidade dos resultados obtidos, restringindo a aplicação do sistema a contextos com infraestrutura semelhante.

3.4 RECOMENDAÇÕES E DIREÇÕES FUTURAS

Com base nos resultados obtidos, recomenda-se a otimização do sistema para melhorar o desempenho em cenários de alta carga, como consultas simultâneas em grande escala. A adoção de técnicas de paralelismo ou a utilização de hardware especializado pode contribuir para essa otimização. Além disso, futuras pesquisas poderiam explorar a aplicação da técnica de RAG em outros contextos legislativos ou áreas que demandem alta precisão e segurança da informação, bem como investigar a integração com outras fontes de dados externas para ampliar o alcance e a relevância das respostas.

ABSTRACT

This project presents a solution that uses Retrieval Augmented Generation (RAG) with private Large Language Models (LLMs). The implementation is built on the Open Web UI platform and integrates Ollama as the LLM engine. The main focus is on Cyber Protection legislation, aiming to provide accurate and concise answers to specific queries by combining data from both public documents, like laws and standards, and private sources, such as security policies and risk management plans. The key tools used in this project include Open

Web UI for managing retrieval and text generation workflows, Ollama for secure and efficient LLM provision, Built-in Embeddings for generating vector representations of content, and ChromaDB for efficient vector storage and retrieval. The RAG approach enables the language model to pull specific information from the uploaded documents, which improves the precision and relevance of the responses. The data source for the RAG process is flexible, allowing adaptation to different situations, which makes the solution versatile and suitable for various applications. This project aims to offer a practical approach to implementing the RAG technique with private LLMs.

Keywords: *Retrieval Augmented Generation (RAG), Large Language Models (LLMs), Open Web UI, Embeddings, Ollama, Vector Storage, Information Retrieval, Document Processing.*

REFERÊNCIAS

MICROSOFT. Overview of Retrieval-Augmented Generation (RAG) for NLP. *Microsoft Learn*, 2024. Disponível em: https://learn.microsoft.com/en-us/azure/applied-ai-services/generative-ai-overview. Acesso em: 22 set. 2024.

LEWIS, Patrick; OGUZ, Barlas; RINOTT, Rachel; RIEDEL, Sebastian; STOYANOV, Veselin. Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks. *Proceedings of Advances in Neural Information Processing Systems (NeurIPS)*, 2020. Disponível em: https://arxiv.org/abs/2005.11401. Acesso em: 28 set. 2024.

ORACLE. Best Practices for Implementing Private Large Language Models. *Oracle Cloud Blog*, 2024. Disponível em: https://blogs.oracle.com/cloud/post/implementing-private-llms-best-practices. Acesso em: 29 set. 2024.

DEVLIN, Jacob; CHANG, Ming-Wei; LEE, Kenton; TOUTANOVA, Kristina. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. *Proceedings of the North American Chapter of the Association for Computational Linguistics (NAACL)*, 2019. Disponível em: https://arxiv.org/abs/1810.04805. Acesso em: 15 out. 2024.

BROWN, Tom; MANN, Benjamin; RYDER, Nick; et al. Language Models are Few-Shot Learners. *Proceedings of Advances in Neural Information Processing Systems (NeurIPS)*, 2020. Disponível em: https://arxiv.org/abs/2005.14165. Acesso em: 25 out. 2024.

IBM. Natural Language Processing: An Introduction. *IBM Cloud Education*, 2024. Disponível em: https://www.ibm.com/cloud/learn/natural-language-processing. Acesso em: 3 out. 2024.

GUU, Kelvin; LEE, Kenton; TURTLE, Zora; YU, Yi; FINE, Jacob. REALM: Retrieval-Augmented Language Model. *Proceedings of the International Conference on Machine Learning (ICML)*, 2020. Disponível em: https://arxiv.org/abs/2002.08909. Acesso em: 6 out. 2024.

GOOGLE CLOUD. Introduction to Vector Databases for NLP Applications. *Google Cloud Documentation*, 2024. Disponível em: https://cloud.google.com/vertex-ai/docs/feature-overview/vector-database. Acesso em: 10 out. 2024.

CISCO. Security Considerations for Large Language Models and Chatbots. *Cisco Cybersecurity Insights*, 2024. Disponível em: https://www.cisco.com/c/en/us/solutions/security/cybersecurity-insights.html. Acesso em: 11 out. 2024.

AMAZON WEB SERVICES (AWS). Building Secure NLP Applications with Amazon SageMaker. *AWS Documentation*, 2024. Disponível em: https://docs.aws.amazon.com/sagemaker/latest/dg/nlp-security.html. Acesso em: 18 out. 2024.

MIN, Sewon; LEWIS, Patrick; HAKKANI-TÜR, Dilek; YIH, Wen-tau. Dense Passage Retrieval (DPR). *Proceedings of the International Conference on Learning Representations (ICLR)*, 2021. Disponível em: https://arxiv.org/abs/2010.03759. Acesso em: 30 out. 2024.

O EMPREGO DE RÁDIOS MILITARES E OS RISCOS QUANTO À ASSINATURA DO SINAL

Ten **LUCAS HENRIQUE** DE SOUZA RAFAEL
S Ten MÁRCIO **R**OBERTO **MARTINS** DE ABREU

RESUMO

Assinaturas de sinal em rádios militares referem-se às características específicas de transmissão que distinguem dos demais equipamentos. Essas assinaturas são um elemento chave da inteligência de sinais, permitindo a identificação e a análise de comunicações militares específicas. Portanto, o emprego de equipamentos rádios com tecnologia militares pode oferecer riscos à segurança em combate, conforme as capacidades de análise dos sinais e Guerra Eletrônica do inimigo.

Palavras-chave: INTELIGÊNCIA DO SINAL, GUERRA ELETRÔNICA, ESPECTRO ELETROMAGNÉTICO

1. INTRODUÇÃO

A inteligência do sinal, ou *Signal Intelligence* (SIGINT) em inglês, deriva-se do espectro eletromagnético e atua na coleta de informações focada na interceptação e análise de sinais de comunicação ou de outros tipos de sinais eletrônicos emitidos por dispositivos, pois atua nas atividades de busca, interceptação, identificação e localização de emissões eletromagnéticas.

O emprego de equipamentos de comunicações militares, ainda que acompanhados de sistemas avançados de segurança da informação, acompanha riscos que afetam à segurança das operações militares. Equipamentos militares possuem tecnologias específicas que caracterizam suas transmissões no espectro eletromagnético, como Salto de Frequência e Sistemas de Estabelecimento Automático de Enlace de Terceira Geração, logo essas emissões são evidências de atividades militares. A identificação das emissões, acompanhada pela localização eletrônica, são fatores de grandes riscos.

2 DESENVOLVIMENTO

2.1 ESPECTRO ELETRMAGNÉTICO

Os sistemas de comunicação por rádio-frequência exploram o espectro eletromagnético para suas transmissões. O espectro eletromagnético não é visível a olho nu, mas a utilização de equipamentos específicos permitem sua visualização, análise de transmissões de rádio e até mesmo a identificação de características desses sinais, como tipos de modulação, criptografia, frequência de utilização e até mesmo recursos avançados de segurança como salto de frequência.

Figura 1- Visualização de uma transmissão de rádio.
Fonte: http://appr.org.br:8905/

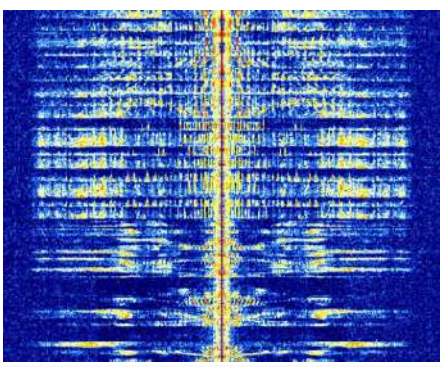
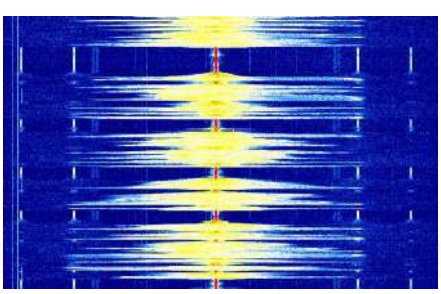


Figura 2L-orFotogrem ipsumafia de uma transmissão em AM.
Fonte: https:www.sigidwiki.com



Fonte: https://www.sigidwiki.com.
Figura 3- Fotografia de uma transmissão em FM.

2.2 DIFERENCIAÇÃO DAS TRANSMISSÕES CIVIS E MILITARES

Através da análise dos sinais no espectro eletromagnético é possível definir se o equipamento transmissor é civil ou um equipamento militar, pois equipamentos militares possuem características específicas. Equipamentos civis utilizam frequências específicas, normalmente são modulações padronizadas como AM (amplitude modulada) ou FM (frequência modulada), suas transmissões não tendem a ser criptografadas ou utilizam criptografia básica (exemplo P25) e não empregam salto de frequência.

Os sinais militares tendem a estar em faixas reservadas para fins militares, utilizam modulações mais complexas, sistemas de estabelecimento automático de link, possuem criptografias complexas e empregam salto de frequência. Além disso, tais sinais possuem padrões de tecnologia proprietária, que são desenvolvidas especialmente para Forças Armadas.

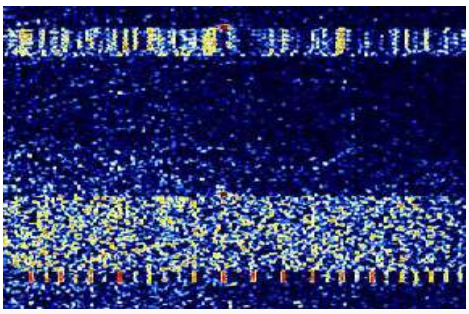


Figura 4 – Fotografia de uma transmissão ALE de Terceira Geração (3G) com padronização military.
Fonte: https://www.sigidwiki.com.

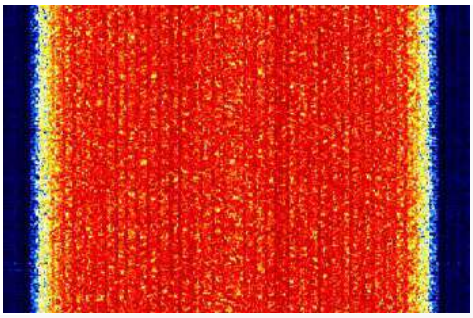


Figura 5 – Fotografia de uma transmissão HF com utilização de protocolos militares.
Fonte: https://www.sigidwiki.com.

2.3 *Direction Finding*: Uma Ferramenta Crucial na Inteligência de Sinais

Direction Finding, ou localização de direção, é uma técnica essencial na guerra eletrônica que desempenha um papel vital na inteligência de sinais . Este processo envolve a determinação da direção de uma fonte de emissão de sinal, como comunicações de rádio, radares ou outras transmissões eletromagnéticas, a partir de um ou mais pontos receptores.

Na guerra eletrônica, a capacidade de identificar a localização de emissores inimigos permite operações militares mais eficazes. Após a confirmação de que o transmissor de RF trata-se de um elemento militar, isso através de confirmações relacionadas à assinatura do sinal, pode-se iniciar medidas para a obtenção de vantagens no Teatro de Operações. Diversas ações podem ser desencadeadas para obtenção de vantagens, como avaliação da capacidade tecnológica inimiga, localização das tropas que operam os equipamentos de comunicações e até mesmo a previsão de planejamentos de contra-ataques inimigos. Esse artigo restringe-se, como exemplo, às ações de localização eletrônica.

A localização eletrônica de transmissores de rádio frequência, tecnicamente conhecida *Direction Finding,* envolve o uso de técnicas e equipamentos especializados para detectar, localizar e identificar a origem de sinais de rádio. Há diversas formas de localizar um transmissor, sendo a triangulação de rádio frequência a mais comum. A triangulação envolve o uso de várias antenas receptoras localizadas em diferentes pontos geográficos. Cada uma dessas antenas mede a intensidade e a direção do sinal recebido do transmissor. Com base nessas medições, as interseções das direções dos sinais indicam a localização aproximada do transmissor.

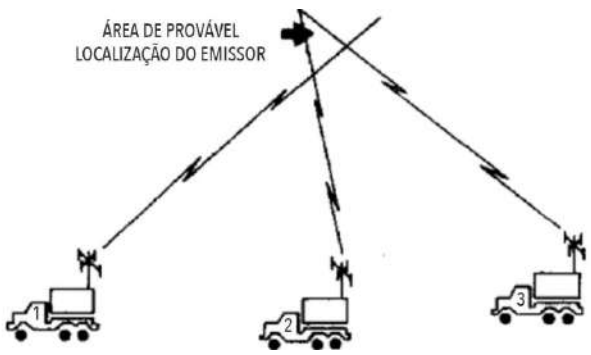


Figura 6 – Ilustração da atividade de *Direction Finding* por triangulação do sinal.
Fonte: https://velhogeneral.com.br/2023/12/04/o-papel-da-guerra-eletronica-de-comunicacao-no-conflito-russia-ucrania/

2.4 RISCOS APÓS A LOCALIZAÇÃO DE ALVOS

Após a localização eletrônica de estruturas militares e alvos compensadores, o que pode ser obtido através da análise de sinais e por sistemas de localização eletrônica, nesse aspecto, os radares são equipamentos muito vulneráveis quanto sua localização eletrônica, devido sua constante emissão de sinais e as características específicas desses sinais. Após as confirmações, diversos tipos de ataques podem ser desencadeados, como ataques aéreos, ataques de artilharia, infiltração, sabotagem de infraestruturas estratégicas e até mesmo a tentativa de captura de materiais de emprego militar.
Um exemplo desse tipo de atuação foi a captura de um Sistema *Krasukha-4* da Rússia, por sua rival Ucrânia, durante o conflito entre os países Rússia e Ucrânia, que se escalou em 24 de fevereiro de 2022.

"Um Krasukha-4 completo consiste em dois veículos, ambos baseados no caminhão KAMAZ-6350 8x8, um com sistema de guerra eletrônica (EW) e outro com módulo de posto de omando."

Figura 7- Sistema russo de radar e posto de commando Krasukha-4.
Fonte: https://galaxiamilitar.es/ucrania-captura-uno-de-los-sistemas-de-guerra-electronica-mas-capaces-de-rusia/

Outro fato que exemplifica, no ano de 2023, militares que operavam em favor da Ucrânia no conflito entre Rússia e Ucrânia decidiram empregar equipamentos civis, pois notaram que a utilização de equipamentos militares resultavam em fogos de artilharia inimiga, segundo depoimento de Leandro Bortolassi, militar que atuou no *front* Rússia-Ucrânia: "A EW no front ucraniano não era consistente, havendo diferenças na intensidade de acordo com a prioridade da região. Em alguns pontos nós mesmos tínhamos rádios designados para captar e ouvir as conversas russas.

Em algumas regiões mais contestadas em que operei, onde haviam combates mais acirrados, o uso dos rádios modelos da Harris como PRC-152 foi deixado de lado.

Esse tipo de rádio apontava um sinal bem específico e intenso para os operadores de Guerra eletrônica russos que entendiam esse sinal como a presença de tropas de operações especiais.

Quando notavam que ali poderiam estar unidades especiais eles intensificavam a vigilância e o ataque sobre nós. Foi aí que boa parte das unidades OpEsp como a nossa decidiu utilizar rádios normais Motorola com criptografia mínima ou nenhuma criptografia.

Era um sacrifício dessa segurança da mensagem para camuflar o nosso sinal em meio as demais unidades convencionais na área de operações.

Ainda com o Motorola, uma técnica básica ainda se valia muito útil: não segurar o PTT continuamente por mais de 5s.

Era nítido que os grupos que não possuíam tal disciplina de rádio eram constantemente alvo de barragem de artilharia e drones FPV.

A complexidade do front se dava pelo fato de que a localização maioria dos Postos de comando nível companhia já era de conhecimento das forças inimigas. Por esse motivo periodicamente o comandante mudava sua posição para tentar evitar atrair atenção". (Bortolassi, 2024)

Figura 8 – Equipamento PRC-152 da L3Harris.
Fonte: https://www.l3harris.com/all-capabilities/falcon-iii-an-prc-152a-wideband-networking-handheld-radio

3 CONCLUSÃO

A utilização de rádios militares em operações táticas e estratégicas, apesar de essencial para a comunicação e coordenação das forças, apresenta riscos significativos devido às características específicas desses equipamentos que podem ser visualizadas no espectro eletromagnético. A principal vulnerabilidade está na possibilidade de detecção dos sinais emitidos, o que pode resultar na localização das tropas e comprometer a segurança e sucesso das operações. Além disso, a suscetibilidade a interferências e a guerra eletrônica adversária pode degradar a qualidade das comunicações ou até mesmo interrompê-las completamente.

Em conclusão, enquanto os rádios militares são ferramentas indispensáveis em campo, sua operação requer uma compreensão profunda dos riscos e a implementação de contramedidas rigorosas para assegurar a eficácia e segurança das comunicações em ambientes hostis.

Abstract

Signal signatures in military radios refer to the specific transmission characteristics that distinguish them from other equipment. These signatures are a key element of signals intelligence, allowing the identification and analysis of specific military communications. The use of military-grade radio equipment can pose security risks in combat, depending on the enemy's signal analysis and electronic warfare capabilities.

Keywords: *SIGNAL INTELLIGENCE, ELECTRONIC WARFARE, ELECTROMAGNETIC SPECTRUM*

4 REFERÊNCIAS

POISEL, Richard. **Introduction to Communication Electronic Warfare Systems**. Boston: Artech House, 2002. 573 p.

BRASIL. Exército. Estado-Maior. EB20-MC-10.207 Inteligência. 1. Ed. Brasília, 2015.

BRASIL. Exército. Estado-Maior. EB70-MC-10.201 A Guerra Eletrônica na Força Terrestre. 1. ed. Brasília, DF, 2019.

BRASIL. Exército. Estado-Maior. EB70-MC-10.247 A Guerra Eletrônica nas Operações. 1. Ed. Brasília, 2020.

BORTOLASSI, Leandro. Depoimento pessoal. Brasília-DF 2024.

DESENVOLVIMENTO E ANALISE DE GESTÃO DE INCIDENTES E SEGURANÇA
DESENVOLVIMENTO DE UMA FERRAMENTA DE GESTÃO DE INCIDENTES DE SEGURANÇA: ANÁLISE DO EMPREGO DA FERRAMENTA THEHIVE EM AMBIENTE SIMULADO

CAP LUÍS HENRIQUE ALVES **VIEIRA**
CAP HAMILTON RODRIGO GOMES DO AMARAL **SANTIAGO** DE ALMEIDA
CAP **FÁBIO** HENRIQUE **DATOLLA**

RESUMO

Este trabalho descreve o processo de desenvolvimento de uma ferramenta voltada para a gestão eficiente de incidentes de segurança da informação em ambientes corporativos. A crescente ameaça de ataques cibernéticos exige que as organizações adotem soluções para monitoramento, registro e mitigação de incidentes de maneira centralizada e eficaz. A ferramenta proposta inclui um sistema de monitoramento em tempo real, registro centralizado de incidentes, além de ferramentas para análise e respostas rápidas já pré estabelecidas. Os testes realizados em um ambiente simulado demonstraram a eficácia da solução em reduzir o tempo de resposta e melhorar a eficiência na gestão de incidentes.

***Palavras-chave**: Gestão de Incidentes, Segurança da Informação, Monitoramento, Resposta a Incidentes.*

1 INTRODUÇÃO

A transformação digital trouxe benefícios significativos, mas também aumentou as ameaças à segurança da informação, como ataques cibernéticos e vazamento de dados. Esses incidentes exigem respostas rápidas e eficazes, tornando essencial a implementação de ferramentas que auxiliem na gestão centralizada e organizada dos incidentes de segurança. Neste contexto cresce a importância da eficácia na gestão de incidentes, haja vista, a utilização massiva de serviços online de todas as naturezas que devem estar "expostos à internet", com disponibilidade diuturna e com informações precisas confiáveis e ágeis.

Muitas empresas enfrentam desafios para a adoção de soluções eficazes devido a custos elevados e falta de expertise, resultando em uma gestão fragmentada e reativa dos incidentes. Esse cenário aumenta os riscos de danos aos sistemas e dados corporativos, evidenciando a necessidade de ferramentas acessíveis e eficientes.

Este trabalho propõe o desenvolvimento de uma ferramenta que permita monitorar, registrar e responder a incidentes de segurança de forma centralizada e em tempo real. A ferramenta busca melhorar a eficiência na detecção e tratamento de incidentes, tornando o processo mais ágil e adequado às necessidades das empresas.

1.1 CONTEXTUALIZAÇÃO DO ESTUDO

Com o aumento da dependência tecnológica, as ameaças à segurança da informação têm crescido de forma alarmante. Empresas de diferentes setores enfrentam, diariamente, tentativas de ataques cibernéticos que podem comprometer a integridade de suas operações. Nesse cenário, a gestão de incidentes de segurança tornou-se um componente essencial da estratégia de proteção de ativos digitais. Entretanto, muitas organizações ainda carecem de ferramentas adequadas para monitorar e gerenciar esses incidentes de forma eficiente e centralizada.

1.2 JUSTIFICATIVA

A relevância de uma ferramenta de gestão de incidentes de segurança se justifica pela necessidade das organizações em melhorar sua capacidade de resposta a ataques. Muitas soluções no mercado apresentam limitações de custo e adaptabilidade para empresas de menor porte ou com infraestrutura heterogênea. A ferramenta proposta visa suprir essa lacuna, oferecendo uma alternativa eficaz e acessível para a detecção e tratamento de incidentes.

1.3 DEFINIÇÃO DO PROBLEMA DE PESQUISA

O problema central abordado por este estudo é a ausência de ferramentas acessíveis e eficientes que permitam a gestão integrada de incidentes de segurança em redes corporativas. A fragmentação de processos e a falta de um sistema de monitoramento contínuo levam a respostas ineficazes e, muitas vezes, tardias a incidentes de segurança.

1.4 OBJETIVOS DA PESQUISA

O objetivo geral deste trabalho é desenvolver uma ferramenta que centralize e otimize a gestão de incidentes de segurança. Os objetivos específicos incluem:

- Implementar um sistema de monitoramento em tempo real para detectar incidentes de segurança. De início, focando em um ponto específico de vulnerabilidade, de forma a iniciar e desenvolver esta ferramenta, para que se torne exequível no tempo disponível, funcional e prática.
- Desenvolver um módulo centralizador para registro e acompanhamento de incidentes.
- Definir procedimentos para a análise e tratamento de incidentes com base em níveis de criticidade.
- Avaliar o desempenho da ferramenta em um ambiente de testes simulados.

1.5 ESTRUTURA DO CONTEÚDO ESCRITO

Este trabalho está dividido nas seguintes seções:

- **Seção 1**: Introdução, onde são apresentados o contexto, a justificativa, a definição do problema e os objetivos do estudo.
- **Seção 2**: Desenvolvimento, que inclui a revisão da literatura, metodologia e análise de dados.
- **Seção 3**: Discussão dos resultados obtidos com a ferramenta desenvolvida.
- **Seção 4**: Conclusão, com as considerações finais e sugestões de futuras melhorias.

2. DESENVOLVIMENTO

A gestão de incidentes de segurança é uma atividade fundamental em um cenário digital cada vez mais vulnerável a ataques cibernéticos. As instituições enfrentam grandes dificuldades para identificar e reagir a incidentes, em razão do aumento contínuo de dados gerados por sistemas de vigilância e da sofisticação das ameaças atuais. Nesse cenário, a automação da resposta a incidentes se torna indispensável, possibilitando que as equipes de segurança atuem de maneira rápida e eficiente, reduzindo os efeitos adversos de possíveis falhas. Ferramentas como TheHive e Cortex surgem como soluções inovadoras que aprimoram os fluxos de trabalho e fortalecem a colaboração entre os especialistas em segurança.

O TheHive proporciona uma plataforma colaborativa que simplifica a gestão de incidentes, possibilitando que as equipes troquem informações em tempo real e tratem casos de maneira organizada. Sua interface amigável torna a criação e a atribuição de tarefas mais eficazes. O Cortex, funcionando como o “cérebro” do TheHive, automatiza análises e respostas, conectando diversas APIs e serviços que asseguram uma rápida ação em face de ameaças. Essa integração entre as duas ferramentas não só facilita uma resposta mais rápida, mas também permite uma análise mais detalhada dos incidentes, com a

coleta de dados relevantes de forma automática, promovendo decisões embasadas. Ademais, a colaboração e a troca de conhecimento são essenciais para o aprimoramento contínuo das práticas de segurança. A utilização do TheHive e do Cortex não só potencializa a resposta a incidentes, mas também cria um ambiente propício para que as equipes aprendam com cada evento, registrando e analisando ocorrências anteriores. Essa metodologia contribui para o desenvolvimento de um banco de dados de conhecimento que pode ser consultado em situações futuras, aumentando a prontidão e resiliência das organizações diante de novas ameaças.

Assim, a adoção dessas ferramentas representa um avanço significativo na gestão de segurança, garantindo que as empresas estejam melhor equipadas para enfrentar os desafios do cenário digital contemporâneo.

2.1 REVISÃO DA LITERATURA

A automatização da resposta a incidentes de cibersegurança tem sido destacada na literatura acadêmica, refletindo o aumento das ameaças digitais e a necessidade de processos de segurança mais eficazes. A resposta a incidentes visa identificar, analisar, mitigar e prevenir eventos que possam afetar a integridade, segurança e disponibilidade da informação dentro das organizações. Inicialmente, estes processos eram manuais, com analistas investigando os incidentes separadamente, resultando muitas vezes em respostas lentas e ineficazes. No entanto, a crescente complexidade dos ataques e o aumento do volume de dados processados exigiram o desenvolvimento de modelos de resposta automatizados.

A literatura enfatiza a importância do ciclo de vida da resposta a incidentes, incluindo as fases de preparação, identificação de ameaças, contenção, remoção e recuperação. Este modelo é essencial para coordenar esforços durante e após um incidente, promovendo uma abordagem estruturada para minimizar os danos. Killcrece et al (2003) sugerem que a integração de tecnologias no ciclo de vida de resposta a incidentes é importante para aumentar a eficiência. A automação surge assim como uma ferramenta capaz não só de acelerar estes processos, mas também de garantir maior precisão e consistência na resposta a incidentes. À medida que a frequência e a complexidade dos ataques cibernéticos aumentaram, a automação tornou-se uma necessidade, especialmente devido à falta de profissionais de segurança qualificados.

De acordo com Grobauer et al. (2010),a automação permite que tarefas operacionais e repetitivas sejam executadas de forma mais rápida e com menos erros, permitindo que os analistas de segurança se concentrem em atividades mais estratégicas.

A literatura discute frequentemente plataformas de automação de segurança e resposta a incidentes (SOAR), que integram diferentes ferramentas e processos em uma única interface. Estas plataformas permitem uma detecção e resposta mais rápida às ameaças, otimizando a detecção (MTTD) e o tempo de resposta (MTTR),conforme destacado pela Gartner (2017).

Entre as soluções SOAR descritas na literatura, a integração das ferramentas TheHive e Cortex vem ganhando atenção. O TheHive é uma plataforma de gerenciamento de incidentes e o Cortex automatiza a análise e execução de ações em resposta a incidentes. Estas ferramentas são particularmente valorizadas pela sua natureza de código aberto, flexibilidade e ampla capacidade de integração com outras soluções de segurança, conforme discutido pelo OpenSOC (2019). TheHive e Cortex se diferenciam de outras plataformas proprietárias pela capacidade de serem customizadas e adaptadas a uma variedade de ambientes empresariais, sejam eles de grande ou médio porte.

A integração das ferramentas TheHive e Cortex é amplamente reconhecida por melhorar a automação da resposta a incidentes de segurança cibernética. Semelhante a Binalay et al (2018),esta integração fornece uma solução robusta para gerenciar e processar as grandes quantidades de dados gerados durante a resposta a incidentes. O Cortex tem a capacidade de realizar ações automatizadas em escala, facilitando a análise de arquivos

suspeitos, a verificação da reputação de domínios e endereços IP e a execução de manuais automatizados de prevenção de ameaças em tempo real. Outro aspecto relacionado é a capacidade de personalizar modelos de incidentes no TheHive. Isto padroniza o processo de resposta, melhora a colaboração entre as equipes de segurança e ajuda a criar uma base de conhecimento baseada em incidentes anteriores. Vilasa et al. (2020) descobriram que automatizar e integrar o Cortex com outros sistemas de segurança, como firewalls e soluções de inteligência contra ameaças, pode expandir ainda mais a capacidade de resposta de uma organização e permitir uma defesa mais proativa e eficaz.

Apesar dos benefícios, a literatura também identifica desafios na implementação da automação da resposta a incidentes. Um dos principais problemas está na configuração das ferramentas de automação. Schreiber (2021) aponta que uma configuração inadequada pode resultar em falsos positivos ou falsos positivos, reduzindo a eficiência do sistema e expondo as organizações a riscos adicionais. Esse problema pode ocorrer devido a regras mal definidas ou soluções desajustadas e pode impactar diretamente sua capacidade de detectar e conter ameaças. Outro desafio diz respeito à dependência excessiva da automação. Embora as ferramentas automatizadas reduzam os tempos de resposta e aumentem a consistência, enquanto While et al (2019) argumentam que a intervenção humana ainda é essencial para a tomada de decisões críticas em incidentes mais complexos. A automação deve, portanto, ser vista como um complemento ao trabalho humano, e não como uma substituição total. A expertise dos analistas ainda é necessária para interpretar os dados e tomar decisões estratégicas, especialmente em cenários que exigem análises mais profundas e contextuais.

A revisão da literatura também revelou diversas lacunas que merecem atenção. Uma delas é a falta de pesquisas sobre a eficácia da integração do TheHive com o Cortex e outras ferramentas integradas em instituições de médio porte. A maioria dos estudos concentra-se em grandes empresas com extensos recursos de TI. No entanto, há pouca pesquisa sobre como usar essas ferramentas de forma eficiente em ambientes com poucos recursos. Outro aspecto pouco discutido é o impacto da automação na formação das equipes de segurança cibernética. Embora a automação reduza as cargas de trabalho manuais, ela pode criar dependências técnicas e reduzir a capacidade do analista de responder a incidentes de forma autônoma.

Automatizar a resposta a incidentes de segurança, especialmente usando ferramentas como TheHive junto ao Cortex, *MISP* e *Wazuh*; pode melhorar significativamente a velocidade e a eficiência das operações de segurança. As plataformas SOAR fornecem um ambiente unificado de detecção e resposta a ameaças, oferecendo benefícios como padronização de processos e tempos de resposta mais rápidos. No entanto, a automação também traz desafios, como a necessidade de configuração cuidadosa e equilíbrio entre tecnologia e intervenção humana. Este estudo visa explorar essas questões mais profundamente, focando na aplicabilidade dessas ferramentas em ambientes de diversos portes.

2.2 MÉTODOS DE PESQUISA

Este estudo visa investigar e analisar o processo de automação de resposta a incidentes de segurança da informação utilizando as ferramentas *TheHive* com *Cortex*, *MISP* e *Wazuh* em um ambiente simulado, aplicando esses conceitos na prática dentro de uma organização de médio porte. Para alcançar os objetivos propostos, foi adotado um método de pesquisa exploratória com uma abordagem mista, envolvendo tanto métodos qualitativos quanto quantitativos.

O estudo foi conduzido em duas etapas principais: uma etapa inicial de pesquisa bibliográfica e uma etapa de experimentação prática. A primeira etapa teve como objetivo revisar a literatura existente sobre a automação de respostas a incidentes de segurança e o uso das ferramentas TheHive juntos com outras ferramentas complementares. Já a segunda etapa consistiu na implementação e avaliação prática das ferramentas em um ambiente de laboratório, simulando cenários de incidentes de segurança para testar a eficiência e eficácia do sistema.

A pesquisa concentrou-se na automação e orquestração de respostas a incidentes em um cenário controlado, permitindo a observação detalhada de como as ferramentas atuam na coleta e análise de dados, na interação com sistemas de terceiros e na execução de tarefas de mitigação e resposta.

A amostra de incidentes de segurança cibernética foi composta por cenários criados artificialmente em um ambiente de laboratório. Esses cenários simulam tentativas de invasão e atividades maliciosas em rede, entre outros tipos de ameaças comuns no ambiente corporativo. Os incidentes foram gerados e configurados para replicar as condições que as ferramentas *TheHive* com *Cortex*, *MISP* e *Wazuh* enfrentaram em um cenário real de resposta a incidentes. Cada incidente foi tratado e analisado pelas ferramentas de forma automatizada, com o objetivo de avaliar sua eficiência e eficácia.

A coleta de dados foi realizada em duas frentes: revisão de literatura e experimentação prática. Na revisão de literatura, foram identificados artigos, livros e relatórios relevantes para o estudo das ferramentas de automação de resposta a incidentes, abordando a utilização de *TheHive* integrados com outras ferramentas, as melhores práticas de segurança cibernética e os desafios enfrentados na automação de respostas. Na fase experimental, foi criado um ambiente de laboratório com as ferramentas *TheHive* com *Cortex*, *MISP* e *Wazuh* instaladas e configuradas para simular incidentes de segurança comuns, como tentativas de invasão, vazamentos de dados e atividades maliciosas em rede. Foram gerados incidentes de segurança de forma artificial, que foram posteriormente tratados pelas ferramentas de maneira automatizada. Os dados coletados incluem tempo de resposta, precisão das análises, taxa de sucesso nas ações de mitigação e nível de colaboração entre as equipes, medido por meio de questionários aplicados aos participantes.

A análise dos dados coletados foi dividida em duas partes. A primeira parte, referente à revisão da literatura, foi conduzida por meio de uma análise qualitativa. Os artigos e publicações foram revisados e categorizados de acordo com temas principais, como "Automação de Respostas a Incidentes", "Ferramentas de SOAR", "Integração de TheHive com *Cortex*, *MISP* e *Wazuh*" e "Melhores Práticas em Segurança da Informação". Essa análise permitiu identificar lacunas no conhecimento e direcionar o estudo para aspectos ainda não completamente explorados. A segunda parte da análise, baseada na experimentação prática, seguiu um método quantitativo. Para isso, foram coletados dados referentes ao desempenho das ferramentas, como o tempo de resposta para cada incidente, o número de incidentes resolvidos sem intervenção humana e a quantidade de falsos positivos detectados. Esses dados foram analisados utilizando estatísticas descritivas, com o objetivo de verificar a eficácia das ferramentas na automação de respostas.

Além disso, foi realizada uma análise qualitativa dos feedbacks fornecidos pelos analistas participantes ao final do experimento. Esses feedbacks foram projetados para obter percepções subjetivas sobre a usabilidade das ferramentas, sua eficácia em comparação com processos manuais e as dificuldades encontradas pelos usuários.

Os métodos descritos neste estudo foram detalhados com o intuito de permitir que outros pesquisadores possam reproduzir a pesquisa em diferentes contextos. A instalação e configuração das ferramentas *TheHive* com *Cortex*, *MISP* e *Wazuh* foram documentadas passo a passo, incluindo as configurações de ambiente de rede, os testes utilizados para a geração dos incidentes simulados e as métricas aplicadas para análise de desempenho. Os incidentes simulados foram configurados para representar cenários de ataque realistas, e as ferramentas foram avaliadas em um ambiente controlado, o que permite que esses experimentos sejam replicados em diferentes organizações ou ambientes de teste, ajustando apenas as variáveis conforme necessário.

Espera-se que este trabalho possa contribuir para o avanço do conhecimento na área de gestão eficiente de incidentes de segurança da informação, além de fornecer um

modelo experimental que possa ser utilizado por outras organizações que desejam implementar ou melhorar suas práticas de segurança cibernética com o uso de ferramentas SOAR.

2.3 APRESENTAÇÃO E ANÁLISE DE DADOS

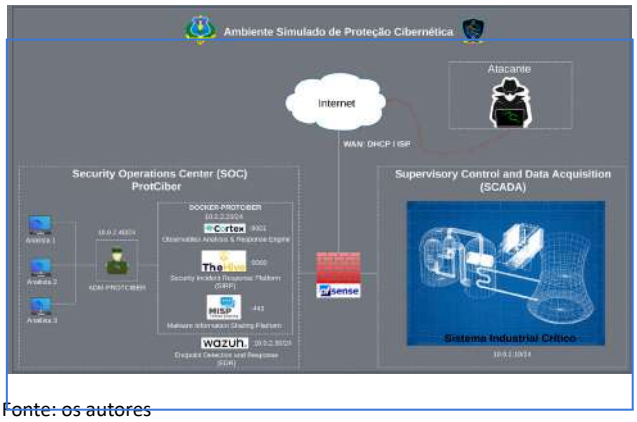
Nesta seção, são apresentados e analisados os dados coletados durante o estudo, que visa avaliar a eficácia da integração da ferramenta *TheHive* com *Cortex*, *MISP* e *Wazuh* em um ambiente simulado de gestão de incidentes de segurança cibernética. O ambiente foi cuidadosamente configurado para refletir um cenário realista, com um Sistema Industrial Crítico (SCADA) e um Security Operations Center (SOC), representando uma estrutura de defesa que monitora e protege ativos sensíveis contra possíveis ameaças externas e internas.

O ambiente simulado, conforme apresentado na figura do estudo, é composto por um SOC com três analistas e ferramentas integradas para detecção e resposta a incidentes. As ferramentas incluem:

- **TheHive**: plataforma central de resposta a incidentes.
- **Cortex**: engine para análise de observáveis, suportando automação de tarefas.
- **MISP**: plataforma para compartilhamento de informações sobre malwares e ameaças.
- **Wazuh**: solução de detecção e resposta a incidentes em endpoints.

Essas ferramentas foram integradas para monitorar, registrar e responder a incidentes de segurança no ambiente simulado, buscando replicar um SOC funcional e interativo.

FIGURA 1 – Ambiente simulado

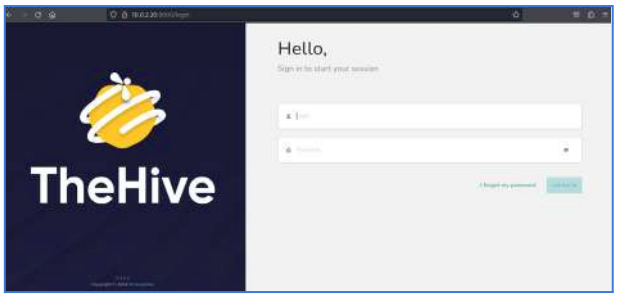


Fonte: os autores

De acordo com Strangebee (2024), o TheHive é uma plataforma abrangente de Resposta a Incidentes de Segurança (SIRP) 4-em-1, projetada para Centros de Operações de Segurança (SOCs), Equipes de Resposta a Incidentes de Segurança de Computadores (CSIRTs), Equipes de Resposta a Emergências de Computadores (CERTs) e profissionais de segurança da informação. Ela oferece um conjunto robusto de recursos que simplificam os fluxos de trabalho de resposta a incidentes, aprimoram a colaboração e permitem uma investigação e mitigação eficazes de ameaças.

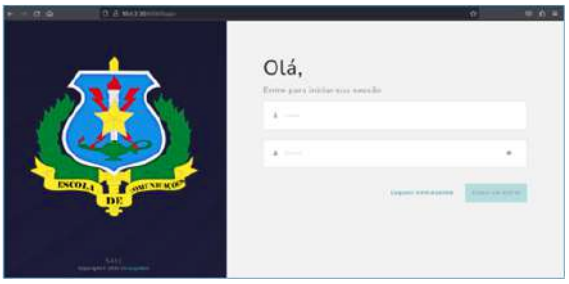
Além disso, o TheHive oferece a possibilidade de adicionar um caso, tarefas, campos personalizados e páginas para organizar e detalhar melhor os incidentes, permitindo uma investigação estruturada e eficiente. Ele facilita a colaboração entre equipes de segurança e fornece uma interface intuitiva para o acompanhamento de atividades e incidentes, tornando-se uma ferramenta essencial para resposta a incidentes e inteligência de ameaças, possibilitando inclusive um histórico dos incidentes existentes na instituição.

FIGURA 2 – Tela de login do TheHive



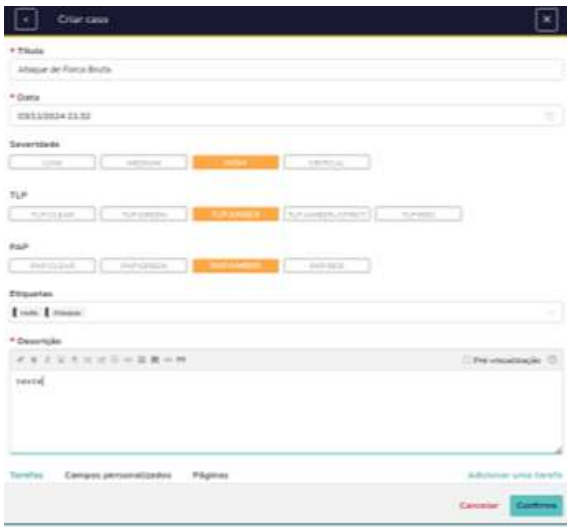
Fonte: os autores

FIGURA 3 – Tela de login do TheHive *customizado*



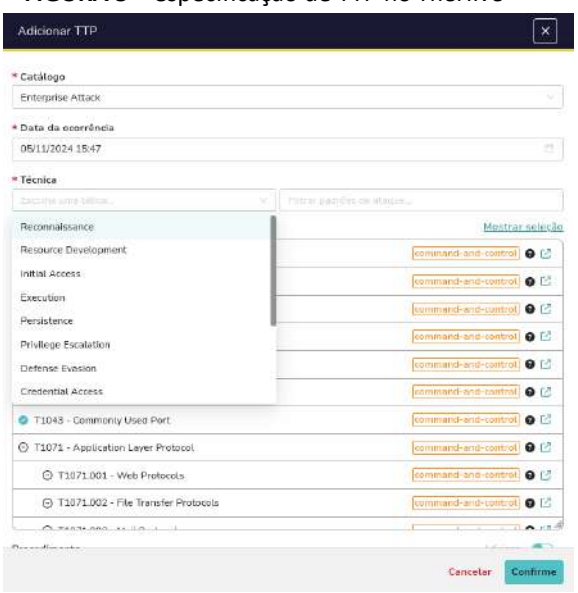
Fonte: os autores

FIGURA 4 – Inserção de incidente no *TheHive*



Fonte: os autores

FIGURA 5 – especificação de TTP no *TheHive*



Fonte: os autores

FIGURA 6 – alertas de incidentes no Sistema SCADA

Fonte: os autores

Durante o período de testes, foram registrados diversos incidentes de segurança, abrangendo tentativas de acesso não autorizado, falhas de autenticação, tentativas de exploração de vulnerabilidades e inúmeros outros incidentes.

De acordo com Wazuh (2024), o Wazuh é uma plataforma de segurança open-source projetada para monitoramento, detecção e resposta a ameaças. Ele oferece uma variedade de recursos que permitem o monitoramento de integridade de arquivos, a análise de logs, a detecção de intrusões e a resposta a incidentes, sendo amplamente utilizado por equipes de segurança da informação para proteger e monitorar infraestruturas de TI.

O teste apresentado evidencia um alerta gerado pelo sistema Wazuh, originado do agente identificado como "SISTEMA-SCADA", conforme registrado na plataforma TheHive. Esse alerta sinaliza a adição de um novo arquivo ao sistema monitorado, o que pode representar uma potencial ameaça, dependendo do contexto operacional. Além disso, o alerta é classificado como uma nova ocorrência, gerada há poucos segundos, sugerindo a detecção recente da atividade. A severidade foi designada com uma classificação de severidade média.

FIGURA 7 – Alerta do Wazuh

Fonte: os autores

Um segundo teste foi realizado, apresentando um alerta gerado pelo sistema Wazuh e originado do agente identificado como "SISTEMA-SCADA", conforme registrado na plataforma TheHive. Esse alerta indica que o serviço Netcat está em escuta para conexões de entrada, o que pode representar uma potencial ameaça, dependendo do contexto operacional. Além disso, o alerta é classificado como uma nova ocorrência, gerada há aproximadamente um minuto, sugerindo a detecção recente da atividade. A severidade foi designada como média.

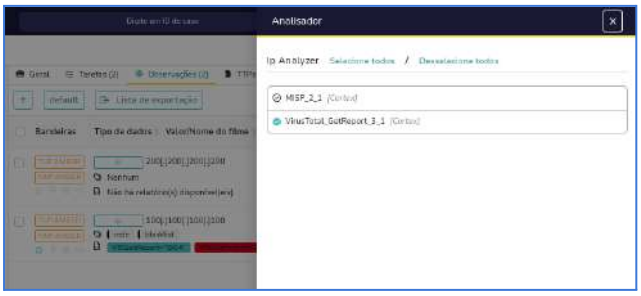
FIGURA 8 – Alerta do Wazuh

Fonte: os autores

De acordo com Strangebee (2024), o Cortex é uma ferramenta complementar ao TheHive que permite a análise automática de indicadores de compromissos e eventos de segurança. Ele fornece uma plataforma para executar uma ampla variedade de análises e gerar relatórios detalhados, facilitando a investigação de incidentes e a resposta a ameaças por parte das equipes de segurança.

Foi realizado um teste onde foi identificado um caso registrado na plataforma TheHive, relacionado ao sistema "SISTEMA-SCADA". Na aba de observáveis, foram analisados dados de IP e domínios através de ferramentas como "MISP 2.1" e "VirusTotal_GetReport_1.1". Essa análise mostra que o sistema está monitorando eventos e ameaças potenciais associadas ao SCADA, com os detalhes do alerta indicando uma atividade monitorada e categorizada recentemente. Esse processo permite avaliar a gravidade e tomar medidas de resposta rápida para mitigar possíveis riscos operacionais ao sistema.

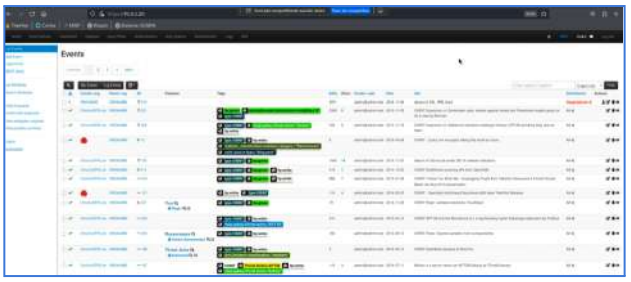
FIGURA 9 – Integração *TheHive* com *Cortex*



Fonte: os autores

De acordo com o MISP Project (2024), o MISP (Malware Information Sharing Platform) é uma plataforma de compartilhamento de informações sobre ameaças de segurança cibernética, que permite a coleta, o armazenamento e a distribuição de indicadores de comprometimento e inteligência de ameaças. Ele é amplamente utilizado por organizações e equipes de segurança para colaborar no combate a ameaças, oferecendo recursos para enriquecer e automatizar a troca de informações sobre ameaças.

FIGURA 10 – Intergração *TheHive* com *MISP*



Fonte: os autores

A imagem apresenta a interface da plataforma MISP (Malware Information Sharing Platform) na seção de eventos, exibindo informações importadas da comunidade para auxiliar na análise e priorização das ações de resposta para os eventos criados no TheHive. Esse monitoramento contínuo permite a identificação de padrões e ameaças recorrentes, promovendo uma postura de defesa mais proativa no sistema SCADA.

A combinação das plataformas TheHive, Cortex, MISP e Wazuh desempenhou um papel essencial na centralização e automação das respostas a incidentes. Quando o Wazuh identifica uma ameaça, ele envia um aviso automaticamente ao TheHive, documentando o caso como um incidente. O Cortex realiza análises automáticas dos dados observáveis e fornece informações pertinentes ao MISP, aumentando assim a base de conhecimento sobre ameaças. Esse processo assegura uma resposta rápida e eficaz, possibilitando que os analistas se concentrem em tarefas mais importantes e diminuindo o tempo de resposta.

A análise dos dados coletados confirma a eficácia do sistema de monitoramento em tempo real, em que todas as ferramentas operam de modo integrado para identificar, registrar e responder a incidentes de segurança. A concentração dos incidentes no TheHive simplificou a monitorização dos casos e a priorização dos mais críticos, com suporte adicional para análises mais aprofundadas e investigações pelo Cortex e MISP. No entanto, foi identificado que o processo ainda envolve intervenções manuais em certas etapas, como a revisão final dos incidentes pelos analistas.

Apesar da eficácia demonstrada por essa abordagem, existem oportunidades para aprimorar a eficiência e a velocidade de resposta.

2.4 DISCUSSÃO DOS RESULTADOS

Os resultados alcançados com a implementação da ferramenta TheHive, integrada ao Cortex, MISP e Wazuh, evidenciam que uma solução centralizada e automatizada para resposta a incidentes é viável e eficaz em um ambiente simulado. O estudo confirmou que, ao integrar essas ferramentas, foi possível identificar e responder a incidentes em tempo real, alcançando os objetivos de monitoramento contínuo e centralização de registros de incidentes. Esse alinhamento com a literatura existente ressalta a importância da automação e da centralização para aprimorar a eficiência nos centros de operações de segurança (SOCs).

A integração possibilitou uma resposta mais ágil e precisa, apresentando benefícios evidentes na priorização de incidentes de acordo com a criticidade, diminuindo a carga manual dos analistas. A utilização do TheHive como módulo centralizador facilitou o monitoramento dos casos, enquanto o Cortex e o MISP enriqueceram as análises com informações sobre ameaças, aprimorando a qualidade das respostas. Esse resultado contribui para o campo da segurança cibernética, demonstrando a eficácia da abordagem integrada para otimizar operações em SOCs.

No entanto, o estudo apresenta limitações. O TheHive, sem outras ferramentas integradas, possui utilidade limitada, funcionando apenas como um repositório de informações e uma plataforma de gestão de incidentes; contudo, quando integrado a outras ferramentas, torna-se uma solução mais robusta para o gerenciamento de incidentes de segurança. O ambiente simulado utilizado neste estudo é menos complexo que uma rede real, e a necessidade de intervenções manuais em certos processos de resposta aponta para oportunidades de melhoria em direção a uma automação mais completa. Além disso, a configuração das ferramentas exige conhecimentos técnicos especializados, o que pode restringir sua aplicabilidade para equipes de segurança com recursos limitados.

Para estudos futuros, recomendamos a avaliação dessa solução em redes maiores e mais complexas, a fim de testar sua escalabilidade e eficácia em ambientes reais. Outra direção relevante é o desenvolvimento de módulos que possibilitem uma automação completa, minimizando ainda mais a intervenção humana e ampliando a agilidade na resposta.

Em resumo, a integração entre TheHive, Cortex, MISP e Wazuh demonstrou ser promissora para a gestão de incidentes, resultando em ganhos significativos em eficiência e eficácia na resposta a incidentes em SOCs. Este estudo enfatiza a relevância da automação e da centralização no enfrentamento de ameaças cibernéticas, além de indicar direções para que investigações futuras expandam o alcance e a aplicabilidade desta solução.

3.1 RESULTADOS

Os resultados da pesquisa demonstram que a utilização integrada das ferramentas TheHive, Cortex, MISP e Wazuh foi efetiva na gestão de incidentes em um ambiente simulado de segurança cibernética. O principal propósito de implantar um sistema de monitoramento em tempo real foi alcançado, possibilitando a identificação e ação ágil diante de incidentes como tentativas de acesso não autorizado, ataques de força bruta e até Implantação de Carga Útil. Além disso, a implementação de um módulo centralizador com TheHive demonstrou-se eficaz para o registro e monitoramento de incidentes, simplificando o processo de priorização com base em sua criticidade. Os procedimentos para o tratamento de incidentes foram executados com êxito, possibilitando uma resposta organizada e eficaz. O desempenho global do sistema demonstrou ser satisfatório para o cenário simulado.

3.2 IMPLICAÇÕES PRÁTICAS E TEÓRICAS

Os resultados deste estudo apresentam implicações práticas e teóricas significativas no campo da segurança cibernética. Do ponto de vista prático, a incorporação de recursos como TheHive, Cortex, MISP e Wazuh evidencia uma estratégia eficaz para automatizar e consolidar a gestão de incidentes em SOCs, aprimorando a eficiência e a prontidão na resposta a ameaças.

Este modelo integrado pode ser implementado por instituições que visam aprimorar seus processos de segurança. No contexto teórico, a pesquisa ressalta a relevância da automação e centralização na mitigação de ameaças cibernéticas, agregando ao conhecimento ao demonstrar que ambientes simulados podem ser eficazes na avaliação do desempenho de soluções de segurança antes de sua implementação em redes reais.

3.3 LIMITAÇÕES E CONSIDERAÇÕES

O estudo apresenta certas limitações metodológicas que necessitam ser levadas em consideração. Inicialmente, é importante ressaltar que o ambiente simulado não reflete completamente a complexidade de uma rede real, o que pode afetar a generalização dos resultados para contextos mais diversos e abrangentes. Ademais, a incorporação das ferramentas demanda conhecimento técnico especializado, o que pode representar um obstáculo à sua implementação em instituições com recursos limitados ou pequenas equipes. O estudo dependeu de intervenções manuais na resposta a incidentes, destacando a importância de uma maior automação para aumentar a independência e eficiência do sistema.

3.4 RECOMENDAÇÕES E DIREÇÕES FUTURAS

Com base nos resultados obtidos, recomendamos que as organizações interessadas em melhorar a gestão de incidentes considerem a implementação de um SOC utilizando uma ferramenta integrada como a utilizada neste estudo.

CERT.BR (2021) recomenda que organizações adotem boas práticas para tratamento de incidentes de segurança, como o uso de plataformas de automação, o que pode auxiliar na mitigação de riscos e no aperfeiçoamento das respostas a ameaças, minimizando impactos e permitindo um acompanhamento contínuo dos incidentes.

Recomendamos pesquisas futuras para avaliar a solução em redes reais e mais complexas e verificar a escalabilidade e robustez do sistema.

Além disso, o desenvolvimento de módulos que automatizam totalmente a resposta a incidentes sem a necessidade de intervenção manual pode melhorar ainda mais a eficácia do sistema.

Estudos comparativos com outras soluções de gerenciamento de incidentes fornecem informações valiosas sobre a relação custo-benefício e a adequação dessas ferramentas para diferentes situações organizacionais.

ABSTRACT

This work describes the development of an external tool for the efficient management of information security incidents in corporate environments. The rising threat of cyber-attacks necessitates that organizations adopt centralized and effective solutions for monitoring, recording, and mitigating incidents. The proposed tool includes a real-time monitoring system, centralized incident logging, and tools for analysis and rapid pre-configured responses. Tests conducted in a simulated environment demonstrated the solution's effectiveness in reducing response time and enhancing efficiency in incident management.

***Keywords**: Incident Management, Information Security, Monitoring, Incident Response.*

REFERÊNCIAS

BINALAY, A. et al. Cortex and TheHive: An Open-Source SOAR Platform for Incident Response Automation. In: *Proceedings of the 2018 International Conference on Cyber Security*, 2018. p. 112-125.

CERT.BR – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Guia de Boas Práticas para Tratamento de Incidentes de Segurança. 2021. Disponível em: https://www.cert.br/docs/guia/. Acesso em: 20 set. 2024.

GARTNER. Market Guide for Security Orchestration, Automation and Response (SOAR). *Gartner Research*, 2017. Disponível em: https://www.gartner.com/en/documents/3760482. Acesso em: 15 out. 2023.

GROBAUER, B.; WALLS, T.; STOECKER, S. Understanding Cloud Computing Vulnerabilities: Automated Incident Response and Security Challenges. *Journal of Information Security*, v. 6, n. 4, p. 298-309, 2010.

KILLCRECE, G. et al. Incident Management in Cybersecurity: Improving Response Efficiency. *Tech Report*, Carnegie Mellon University, 2003.

LOPES, R. V.; MONTONI, M. A. Gestão de Segurança da Informação com Base em ISO/IEC 27001. *Revista Tecnologia e Sociedade*, v. 8, n. 2, p. 43-58, 2013.

MEDEIROS, I. C.; COSTA, F. R.; VELOSO, P. A. S. Segurança em Redes de Computadores: Ataques, Ferramentas e Técnicas de Defesa. *Revista Brasileira de Computação Aplicada*, v. 4, n. 2, p. 89-101, 2012.

MISP PROJECT. MISP Documentation: Overview. Disponível em: https://www.misp-project.org/. Acesso em: 06 out. 2024.

OPENSOC. Open-Source Security Tools: Implementing TheHive and Cortex for Incident Management. *OpenSOC Workshop Report*, 2019. Disponível em: https://www.opensoc.com/report-2019. Acesso em: 20 set. 2023.

ROCHA, S. S.; SOARES, M. S.; ALVES, V. L. A Automação e Orquestração da Resposta a Incidentes com o Uso de TheHive e Cortex. *Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica*, v. 17, n. 3, p. 65-78, 2021.

SCHREIBER, M. Challenges in Automating Incident Response: The Human Factor in Security Automation. *Cyber Defense Review*, v. 6, n. 3, p. 101-119, 2021.

STRANGEBEE. TheHive Overview: Application Stack. Disponível em: https://docs.strangebee.com/thehive/overview/. Acesso em: 06 set. 2024.

VILAÇA, P.; RIBEIRO, T.; SANTOS, A. Enhancing Incident Response with TheHive and Cortex Integration. *Journal of Cybersecurity Engineering*, v. 12, n. 2, p. 55-72, 2020.

WAZUH. Wazuh Documentation: Overview. Disponível em: https://documentation.wazuh.com/. Acesso em: 06 set. 2024.

WHILE, P.; JONES, S.; MITCHELL, C. Human-Centric Incident Response: Limitations of Full Automation in Cybersecurity. *International Journal of Cyber Operations*, v. 8, n. 1, p. 34-49, 2019

ANALISADOR PORTÁTIL DE PENDRIVES COM RASPBERRY PI 4 B: UMA SOLUÇÃO EFICIENTE PARA DETECÇÃO DE AMEAÇAS EM MEMÓRIAS PORTÁTEIS

Ten JEFFERSON **ADINIZ** BORGES FERREIRA
Sgt ANDERSON **LUCIO** GOMES

Resumo: Este trabalho propõe o uso do Raspberry Pi 4 B como base para a construção de um analisador portátil de pendrives, oferecendo uma solução eficiente para a detecção de ameaças em dispositivos de armazenamento portáteis. Utilizando a API do VirusTotal, o Raspberry Pi 4 B, um computador de placa única acessível e versátil, possibilita a monitorização e análise eficaz de dados em dispositivos USB, identificando potenciais ameaças e fortalecendo a segurança da informação. A integração com a API do VirusTotal adiciona uma camada extra de proteção, permitindo a verificação de arquivos contra uma vasta base de dados de malwares conhecidos. Neste artigo, serão exploradas as funcionalidades principais do Raspberry Pi 4 B, discutidas suas vantagens, e apresentados exemplos práticos de sua aplicação na análise de pendrives, ressaltando sua importância como um ativo valioso em infraestruturas de segurança da informação.

Palavras-Chave: Raspberry PI, Pen Drives, Vírus Total

1. INTRODUÇÃO

Na era digital, em que a troca rápida e segura de informações é crucial, a proteção de dados se torna uma preocupação central. Dispositivos de armazenamento portáteis, como pendrives, são amplamente utilizados para transferir dados entre diferentes sistemas. No entanto, essa conveniência está associada a riscos significativos, uma vez que pendrives podem se tornar veículos de disseminação de malwares e outras ameaças cibernéticas.

A detecção de ameaças em memórias portáteis é, portanto, uma medida de segurança indispensável para proteger sistemas e redes de possíveis ataques. Tanto organizações quanto indivíduos necessitam de ferramentas eficazes que permitam a análise rápida desses dispositivos, garantindo que não representem um risco. Nesse contexto, o Raspberry Pi 4 B emerge como uma solução acessível e eficiente. O Raspberry Pi 4 B é um computador de placa única, desenvolvido pela Raspberry Pi Foundation, reconhecido por sua versatilidade e baixo custo, pode ser utilizado como base para a construção de um analisador portátil de pendrives.

A integração da API do VirusTotal ao Raspberry Pi 4 B adiciona uma poderosa camada de segurança. O VirusTotal é um serviço que agrega resultados de múltiplos

mecanismos antivírus e ferramentas de análise de malware, possibilitando uma verificação abrangente de arquivos suspeitos. Ao utilizar essa API, é possível escanear arquivos armazenados em pendrives contra uma extensa base de dados de malwares conhecidos, ampliando significativamente a capacidade de detecção e resposta a ameaças.

Este artigo explora a importância da proteção de dados e sistemas contra as ameaças introduzidas por memórias portáteis. Discutiremos como o Raspberry Pi 4 B, em conjunto com a API do VirusTotal, pode ser utilizado para criar um analisador portátil de pendrives. Além disso, serão apresentadas as vantagens dessa solução, bem como exemplos práticos de sua aplicação, ressaltando sua relevância como um componente crucial em infraestruturas de segurança da informação.

2. DESENVOLVIMENTO

2.1 ARQUITETURA E CONFIGURAÇÃO DO ANALISADOR DE PENDRIVES COM Raspberry pi 4 B

A configuração do Raspberry pi 4 B como um analisador de pendrives começa com a escolha dos componentes de hardware e software. O Raspberry pi 4 B, com sua combinação de tamanho compacto e poder de processamento suficiente, é ideal para esta tarefa. Neste subitem, discutiremos:

Seleção de Hardware as características principais do Raspberry Pi 4 incluem:

- **Processador:** Broadcom BCM2711, um SoC (System on a Chip) que possui uma CPU quad-core ARM Cortex-A72 de 64 bits, com clock de 1,5 GHz.
- **Memória:** Disponível em versões com 2 GB, 4 GB ou 8 GB de memória RAM LPDDR4.
- **Armazenamento:** Utiliza cartões microSD para armazenamento principal, mas também suporta boot por USB, permitindo o uso de SSDs externos para melhorar a performance.
- **Conectividade:** Possui portas USB 3.0 e USB 2.0, Gigabit Ethernet, e conectividade sem fio integrada, incluindo Wi-Fi 802.11ac de banda dupla e Bluetooth 5.0.
- **Vídeo e Gráficos:** Suporta saída de vídeo em 4K a 60 fps através de duas portas micro HDMI, sendo ideal para aplicações de multimídia.
- **Sistema Operacional:** Compatível com várias distribuições de sistemas operacionais baseados em Linux, como o Raspberry Pi OS, além de ser capaz de rodar sistemas operacionais como Ubuntu e até mesmo versões de Windows 10 IoT Core.

O Raspberry Pi 4 é especialmente valorizado por seu equilíbrio entre desempenho e custo, tornando-o uma escolha popular para projetos educacionais, domésticos, industriais e de pesquisa.

Além do Raspberry pi 4 B, é necessário um adaptador USB OTG para conectar os pendrives, uma fonte de alimentação estável, e um cartão microSD com uma capacidade mínima de 16 GB para armazenar o sistema operacional e os arquivos temporários. Dependendo do ambiente de uso, um case protetor pode ser recomendado para proteger o dispositivo durante o transporte.

Instalação do Sistema Operacional: O Raspberry Pi OS (anteriormente conhecido como Raspbian) é a escolha ideal devido à sua compatibilidade e suporte à comunidade. Discutiremos as etapas de instalação do sistema operacional, incluindo o download da imagem, o uso do Raspberry Pi Imager, e as primeiras configurações, como a habilitação do SSH para acesso remoto.

Alimentação: A alimentação do dispositivo será feita por duas baterias 18650 de 2A conectadas em série. Essa configuração fornece uma tensão nominal de 7.4V, o que é adequado para alimentar o Raspberry pi 4 B por um período prolongado. Nota: O tempo de utilização estimado é baseado em uma carga total das baterias e em condições de operação típicas. O uso de periféricos adicionais ou uma carga parcial das baterias pode reduzir esse tempo.

Configuração de Rede: Como a API do VirusTotal requer conexão à internet, abordaremos a configuração da conectividade via Wi-Fi, com foco na conexão ao roteador Wi-Fi do smartphone do usuário. **2.2 INTEGRAÇÃO COM A API DO VIRUSTOTAL**

A integração com a API do VirusTotal é uma das funcionalidades mais poderosas do analisador de pendrives, permitindo uma verificação eficaz de arquivos em busca de ameaças. Este subitem detalha cada etapa do processo:

Registro e Configuração da API:

O primeiro passo para utilizar a API do VirusTotal é o registro no serviço para obtenção de uma chave de API, que será usada para autenticação nas chamadas. Vamos explicar como configurar essa chave no Raspberry Pi, sugerindo o uso de variáveis de ambiente para armazená-la de forma segura, facilitando seu acesso nos scripts e mantendo a segurança dos dados.

Criação de Scripts para Chamadas à API:

Usando Python, vamos demonstrar como criar scripts que automatizam o envio de arquivos armazenados em pendrives para análise no VirusTotal. Serão discutidas as bibliotecas essenciais, como requests, e serão fornecidos exemplos práticos de código que realizam chamadas à API, obtêm relatórios de verificação e processam as respostas, permitindo a identificação de ameaças de maneira eficiente. O foco será em garantir que o processo seja ágil e possa ser facilmente integrado em soluções de segurança maiores.

Limitações da API e Soluções Alternativas: Como a API do VirusTotal impõe limites no número de chamadas por minuto, apresentaremos estratégias para otimizar seu uso. Entre elas, destacamos a verificação seletiva de arquivos com base no hash (por exemplo, SHA-256) para evitar a análise redundante de arquivos já verificados, e o uso de cache local para armazenar resultados temporários. Além disso, alternativas viáveis, como outras APIs de antivírus gratuitas ou de código aberto, que possam complementar o VirusTotal, oferecendo maior flexibilidade na detecção de ameaças e ampliando a cobertura de segurança.

2.3 PROCESSAMENTO E ANÁLISE DE ARQUIVOS

O processamento e a análise dos arquivos são fundamentais para a eficácia do analisador. Neste subitem, abordaremos:

Análise Preliminar de Arquivos: Antes de enviar arquivos para o VirusTotal, o Raspberry Pi pode realizar uma análise preliminar. Discutiremos técnicas para verificar a integridade dos arquivos, identificar extensões suspeitas, e analisar metadados que possam indicar comportamento malicioso, como a presença de scripts autorun.

Uso de Bancos de Dados Locais: Para acelerar o processo de análise, o Raspberry Pi pode utilizar bancos de dados locais de hashes de malwares conhecidos. Explicaremos como atualizar e manter esses bancos de dados, além de como usá-los para comparações rápidas antes de recorrer à API do VirusTotal.

Análise Comportamental e de Padrões: Para arquivos que não correspondem a malwares conhecidos, discutiremos como implementar técnicas de análise comportamental. Isso pode incluir a execução de scripts em um ambiente sandbox no Raspberry Pi para observar comportamentos anômalos, como tentativas de se conectar à internet ou modificar arquivos do sistema.

Alertas de Ameaças: Após a análise, o Raspberry Pi indicará a presença de ameaças por meio de um sistema de LEDs. Um LED verde acenderá para indicar que o pendrive está limpo, enquanto um LED vermelho indicará a detecção de uma ameaça. Abordaremos como configurar esses LEDs para reagirem em tempo real aos resultados da análise, garantindo uma sinalização clara e imediata do status do dispositivo.

2.4 IMPLEMENTAÇÃO E TESTES PRÁTICOS

A implementação prática da solução é crucial para validar sua eficácia. Este subitem está focado em:

Controlar os LEDs conectados ao Raspberry Pi durante o processo de verificação de pendrives, você pode usar a biblioteca **GPIO**

do Python, que permite controlar os pinos GPIO para ligar e desligar os LEDs.

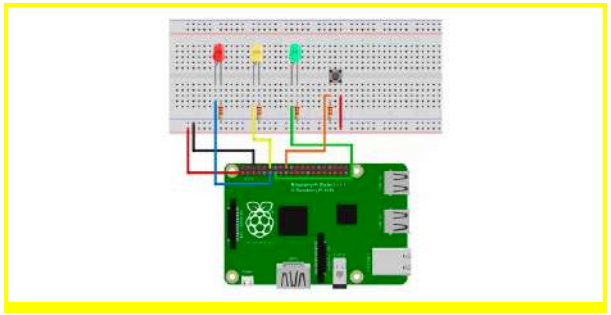
Os LEDs estão conectados aos pinos GPIO do Raspberry Pi funcionam da seguinte maneira:

O **LED amarelo** acende durante a verificação.

Quando a verificação terminar:

O **LED vermelho** acende se houver uma ameaça.

O **LED verde** acende se o pendrive estiver seguro.



O passo a passo da implementação é o seguinte:

Atualize o sistema:

```bash
sudo apt update
sudo apt upgrade
```

Instalar o Python e pip (caso não esteja instalado):

```bash
sudo apt install python3 python3-pip
```

2. Obtenção da API Key do VirusTotal

Para usar a API do VirusTotal, você precisa obter uma chave de API gratuita ou paga. Basta criar uma conta no VirusTotal, acessar o painel de controle e copiar sua chave de API.

3. Instalar Bibliotecas Necessárias

Para fazer chamadas HTTP e interagir com a API do VirusTotal, você usará a biblioteca requests. Instale-a usando o pip:

```bash
pip3 install requests
```

4. Criar Script em Python para Chamadas à API

Agora, você pode criar um script que envia arquivos de pendrives para análise no VirusTotal. Aqui está um exemplo de script básico:

```python
import os
import requests

# Sua chave de API do VirusTotal
API_KEY = 'SUA_CHAVE_API_AQUI'

# URL para enviar o arquivo à API do VirusTotal
url = 'https://www.virustotal.com/vtapi/v2/file/scan'

# Função para enviar o arquivo
def enviar_arquivo_virus_total(file_path):
    # Verifica se o arquivo existe
    if not os.path.isfile(file_path):
        print(f'Arquivo {file_path} não encontrado.')
        return

    # Dados para a API
    params = {'apikey': API_KEY}
    files = {'file': (file_path, open(file_path, 'rb'))}

    # Faz a chamada à API
    response = requests.post(url, files=files, params=params)

    # Verifica a resposta da API
    if response.status_code == 200:
        print(f'Arquivo enviado com sucesso. Resposta: {response.json()}')
    else:
        print(f'Erro ao enviar o arquivo. Código HTTP: {response.status_code}')

# Caminho do arquivo no pendrive para análise
caminho_do_arquivo = '/media/pi/pendrive/nome_do_arquivo.ext'

# Envia o arquivo para o VirusTotal
enviar_arquivo_virus_total(caminho_do_arquivo)
```

5. Verificar o Status da Análise

Depois de enviar o arquivo, você pode verificar o status da análise usando outro endpoint da API. Aqui está como fazer isso:

```python
import requests

# URL para verificar o relatório da API
url_report = 'https://www.virustotal.com/vtapi/v2/file/report'

# Função para obter o relatório de análise
def obter_relatorio_virus_total(resource_id):
    params = {'apikey': API_KEY, 'resource': resource_id}

    response = requests.get(url_report, params=params)

    if response.status_code == 200:
        json_response = response.json()
        print(f"Relatório recebido: {json_response}")
        # Processa os resultados conforme necessário
    else:
        print(f"Erro ao obter o relatório. Código HTTP: {response.status_code}")

# Resource ID ou SHA-256 do arquivo para buscar o relatório
resource_id = 'ID_DO_ARQUIVO_AQUI'
obter_relatorio_virus_total(resource_id)
```

6. Considerações sobre Limites da API

- A versão gratuita do VirusTotal permite até 4 solicitações de análise por minuto.
- Para evitar atingir o limite, você pode implementar verificação pelo hash do arquivo antes de fazer uma nova solicitação.
- Armazenar localmente os resultados (cache) também pode ajudar a evitar enviar o mesmo arquivo repetidamente.

7. Execução Automática no Raspberry Pi

O Raspberry Pi pode monitorar automaticamente os pendrives conectados e envie os arquivos para o VirusTotal, com um script que verifica novos dispositivos USB conectados e inicia o processo automaticamente.

```python
import os
import time

# Diretório onde os pendrives são montados no Raspberry Pi
usb_directory = '/media/pi/'

def verificar_dispositivos_usb():
    while True:
        dispositivos = os.listdir(usb_directory)
        if dispositivos:
            print(f"Dispositivo detectado: {dispositivos}")
            # Itera sobre os arquivos do pendrive e envia para análise
            for dispositivo in dispositivos:
                caminho_do_dispositivo = os.path.join(usb_directory, dispositivo)
                for root, dirs, files in os.walk(caminho_do_dispositivo):
                    for file in files:
                        file_path = os.path.join(root, file)
                        enviar_arquivo_virus_total(file_path)
        else:
            print("Nenhum pendrive detectado.")
        time.sleep(10)

# Verifica dispositivos USB constantemente
verificar_dispositivos_usb()
```

Os LEDs estão conectados aos pinos GPIO do Raspberry Pi. A ideia é o **LED amarelo** acende durante a verificação. Quando a verificação terminar:O **LED vermelho** acende se houver uma ameaça. O **LED verde** acende se o pendrive estiver seguro.

Configurando os LEDs com GPIO:

1. **Instalar a biblioteca RPi.GPIO:** Se ainda não tiver a biblioteca instalada, instale-a com o seguinte comando:

```bash
sudo apt install python3-rpi.gpio
```

```python
import RPi.GPIO as GPIO
import time
import requests
import os

# Configuração dos pinos GPIO para os LEDs
LED_VERDE = 17   # Pino GPIO para o LED verde
LED_AMARELO = 27  # Pino GPIO para o LED amarelo
LED_VERMELHO = 22  # Pino GPIO para o LED vermelho

# Configuração inicial dos pinos GPIO
GPIO.setmode(GPIO.BCM)
GPIO.setup(LED_VERDE, GPIO.OUT)
GPIO.setup(LED_AMARELO, GPIO.OUT)
GPIO.setup(LED_VERMELHO, GPIO.OUT)

# Função para limpar os LEDs (desligar todos)
def limpar_leds():
    GPIO.output(LED_VERDE, GPIO.LOW)
    GPIO.output(LED_AMARELO, GPIO.LOW)
    GPIO.output(LED_VERMELHO, GPIO.LOW)

# Configuração da API VirusTotal
API_KEY = 'SUA_CHAVE_API_AQUI'
url = 'https://www.virustotal.com/vtapi/v2/file/scan'
url_report = 'https://www.virustotal.com/vtapi/v2/file/report'
```

```python
# Função para enviar o arquivo para o VirusTotal
def enviar_arquivo_virus_total(file_path):
    limpar_leds()
    print("Iniciando verificação...")

    # Acende o LED amarelo durante a verificação
    GPIO.output(LED_AMARELO, GPIO.HIGH)

    # Envia o arquivo para o VirusTotal
    if not os.path.isfile(file_path):
        print(f"Arquivo {file_path} não encontrado.")
        return

    params = {'apikey': API_KEY}
    files = {'file': (file_path, open(file_path, 'rb'))}
    response = requests.post(url, files=files, params=params)

    if response.status_code == 200:
        json_response = response.json()
        resource_id = json_response['resource']
        # Faz a verificação do relatório
        time.sleep(30)  # Espera 30 segundos para que o relatório seja gerado
        return obter_relatorio_virus_total(resource_id)
    else:
        print(f"Erro ao enviar o arquivo. Código HTTP: {response.status_code}")
```

```python
# Função para monitorar os dispositivos USB montados
def monitorar_pendrive():
    usb_directory = '/media/pi/'  # Diretório onde os pendrives são montados
    dispositivos_montados = set()

    while True:
        dispositivos_atual = set(os.listdir(usb_directory))

        # Detecta novos dispositivos conectados
        novos_dispositivos = dispositivos_atual - dispositivos_montados
        if novos_dispositivos:
            print(f"Novo pendrive detectado: {novos_dispositivos}")
            for dispositivo in novos_dispositivos:
                caminho_do_dispositivo = os.path.join(usb_directory, dispositivo)
                for root, dirs, files in os.walk(caminho_do_dispositivo):
                    for file in files:
                        file_path = os.path.join(root, file)
                        enviar_arquivo_virus_total(file_path)

        dispositivos_montados = dispositivos_atual

        # Verifica a cada 5 segundos por novos pendrives
        time.sleep(5)

# Função principal
try:
    limpar_leds()
    monitorar_pendrive()
except KeyboardInterrupt:
    print("Programa interrompido.")
finally:
    limpar_leds()
    GPIO.cleanup()
```

: A função monitorar_pendrive() verifica constantemente o diretório /media/pi/, onde os pendrives são montados automaticamente no Raspberry Pi. Quando detecta um novo dispositivo, inicia o processo de verificação dos arquivos contidos no pendrive.

Verificação de Arquivos: Para cada pendrive detectado, o código caminha pelas pastas e arquivos contidos nele e envia cada arquivo para a análise no VirusTotal.

Controle dos LEDs:

- O **LED amarelo** acende durante a verificação.
- Se for detectada uma ameaça, o **LED vermelho** acende.
- Se o pendrive estiver seguro, o **LED verde** será ativado.

Loop de Monitoramento: O loop verifica novos dispositivos a cada 5 segundos e atualiza a lista de dispositivos montados, para garantir que detecte pendrives recém-conectados.

Executar o Script: Salve o script em um arquivo Python, por exemplo verificador_pendrive.py, e execute no Raspberry Pi:

Conecte um pendrive e observe o comportamento dos LEDs. Durante a verificação, o LED amarelo acenderá, e quando o processo for concluído, o LED vermelho ou verde será ativado, dependendo dos resultados.

2.5 VANTAGENS E DESAFIOS DA SOLUÇÃO

Vantagens: Destacamos as principais vantagens do uso do Raspberry pi 4 B como analisador de pendrives, incluindo seu custo acessível, sua portabilidade, e a facilidade de configuração e uso, ele pode ser integrado em infraestruturas de segurança maiores e sua utilidade como ferramenta de resposta a incidentes.

Desafios Técnicos: as limitações do hardware, como a capacidade de processamento e armazenamento, e como isso pode afetar a análise de grandes volumes de dados ou de arquivos complexos. A conectividade de rede limitada em ambientes com pouca infraestrutura também será considerada.

Manutenção e Atualizações: Manter a eficácia da solução requer atualizações frequentes tanto do software quanto das bases de dados de malwares. As estratégias para garantir que o Raspberry Pi esteja sempre atualizado e preparado para detectar novas ameaças, incluindo a automação de atualizações e a verificação de integridade do sistema.

Escalabilidade e Adaptação: Finalmente, a solução pode ser escalada para uso em ambientes maiores ou adaptada para funções adicionais, como a análise de outros tipos de dispositivos USB, como discos rígidos externos ou smartphones.

CONCLUSÃO

O uso do Raspberry pi 4 B como base para um analisador portátil de pendrives demonstra ser uma solução eficaz e acessível para a detecção de ameaças em dispositivos de armazenamento portáteis. Ao integrar a API do VirusTotal, o dispositivo é capaz de realizar verificações profundas e abrangentes, protegendo sistemas e redes contra malwares conhecidos. A configuração do dispositivo para se conectar ao Wi-Fi roteado do smartphone do usuário garante mobilidade e flexibilidade, permitindo que a análise de pendrives seja realizada em diversos ambientes sem a necessidade de infraestrutura adicional.

A simplicidade do sistema de alertas por LEDs, que indica a presença ou ausência de ameaças de maneira direta e visual, torna a solução prática e fácil de usar, tanto para profissionais de segurança da informação quanto para usuários menos experientes. A escolha de utilizar baterias 18650 em série para a alimentação do dispositivo também assegura um tempo de operação prolongado, fazendo com que o analisador seja confiável e eficiente mesmo em situações onde o acesso à energia elétrica é limitado.

Este projeto destaca a importância de soluções de segurança cibernética portáteis e acessíveis, especialmente em um cenário onde a mobilidade é cada vez mais valorizada.

Com as melhorias e adaptações discutidas ao longo deste artigo, o analisador de pendrives com Raspberry pi 4 B tem opotencial de se tornar uma ferramenta essencial em infraestruturas de segurança, fornecendo uma defesa robusta contra ameaças cibernéticas provenientes de dispositivos USB.

REFERÊNCIAS BIBLIOGRÁFICAS

RASPBERRY PI FOUNDATION, **Getting started with your Raspberry Pi**. Disponível em:

RASPBERRY PI FOUNDATION. *Getting started with Raspberry Pi*. Disponível em: https://www.raspberrypi.com/documentation/computers/getting-started.html/. Acesso em: 26 ago. 2024.

PYPI. *virustotal-api 1.1.11*. Disponível em: https://pypi.org/project/virustotal-api/. Acesso em: 27 ago. 2024.

VIRUSTOTAL. *VirusTotal API v2.0 - Getting started*. Disponível em: https://docs.virustotal.com/v2.0/reference/getting-started. Acesso em: 27 ago. 2024. PYPI. *virustotal-python 0.1.2*. Disponível em: https://pypi.org/project/virustotal-python/. Acesso em: 27 ago. 2024.

FORUMS. *Raspberry Pi - Monitoring USB device connections*. Disponível em: https://forums.raspberrypi.com/viewtopic.php?t=318933. Acesso em: 27 ago. 2024.

MAKERHERO. *Projetos com Raspberry Pi*. Disponível em: https://www.makerhero.com/blog/projetos-com-raspberry-pi/. Acesso em: 4 set. 2024.

SILVA, João P. *Detecção de Ameaças Cibernéticas em Dispositivos USB*. 2022. Dissertação (Mestrado em Segurança da Informação) – Universidade Federal de São Paulo, São Paulo, 2022.

Anexo A - Sequência de instalação do Virus Total no

```
$ pip install virustotal-api

from __future__ import print_function
import json
import hashlib
from virus_total_apis import PublicApi as
VirusTotalPublicApi

API_KEY = 'Sign-Up for API Key at
virustotal.com'

EICAR =
"X5O!P%@AP[4\PZX54(P^)7CC)7}$EIC
AR-STANDARD-ANTIVIRUS-TEST-FILE!
$H+H*".encode('utf-8')
EICAR_MD5 =
hashlib.md5(EICAR).hexdigest()

vt = VirusTotalPublicApi(API_KEY)

response =
vt.get_file_report(EICAR_MD5)
print(json.dumps(response,
sort_keys=False, indent=4))

{
   "response_code": 200,
   "results": {
      "scan_id":
"275a021bbfb6489e54d471899f7db9d16
63fc695ec2fe2a2c4538aabf651fd0f-1397
510237",
```

```
    "sha1":
"3395856ce81f2b7382dee72602f798b64
2f14140",
    "resource":
"44d88612fea8a8f36de82e1278abb02f",
    "response_code": 1,
    "scan_date": "2014-04-14 21:17:17",
    "permalink":
"https://www.virustotal.com/file/275a021b
bfb6489e54d471899f7db9d1663fc695ec2
fe2a2c4538aabf651fd0f/analysis/139751
0237/",
    "verbose_msg": "Scan finished, scan
information embedded in this object",
    "sha256":
"275a021bbfb6489e54d471899f7db9d16
63fc695ec2fe2a2c4538aabf651fd0f",
    "positives": 49,
    "total": 51,
    "md5":
"44d88612fea8a8f36de82e1278abb02f",
    "scans": {
      "Bkav": {
        "detected": true,
        "version": "1.3.0.4959",
        "result": "DOS.EiracA.Trojan",
        "update": "20140412"
      },
      "MicroWorld-eScan": {
        "detected": true,
        "version": "12.0.250.0",
        "result": "EICAR-Test-File",
        "update": "20140414"
      },
      "nProtect": {
        "detected": true,
        "version": "2014-04-14.02",
        "result": "EICAR-Test-File",
        "update": "20140414"
      },
      ...<snip>...
      "AVG": {
        "detected": true,
        "version": "13.0.0.3169",
        "result": "EICAR_Test",
        "update": "20140414"
      },
      "Panda": {
        "detected": true,
        "version": "10.0.3.5",
        "result":
"EICAR-AV-TEST-FILE",
        "update": "20140414"
      },
      "Qihoo-360": {
        "detected": true,
        "version": "1.0.0.1015",
        "result": "Trojan.Generic",
        "update": "20140414"
      }
    }
  }
}


$ ./tests
```

CONSCIENTIZAÇÃO DE PHISHING: ESTRATÉGIAS E IMPACTO NA SEGURANÇA CIBERNÉTICA

Ten MATHEUS AGUIAR **SELLA**
Ten **BRENDO BASTOS** MACEDO
Ten MATHEUS **MARQUES** DA SILVA DA PAZ BATISTA

RESUMO

Esta pesquisa buscou a conscientização acerca dos riscos provenientes de ameaças Phishing e, para tanto, buscou-se a implementação de uma ferramenta capaz de testar o grau de exposição de um determinado grupo de usuários a este tipo de ameaça. Foi realizada uma pesquisa aplicada de caráter exploratório com abordagem qualitativa, utilizando-se de uma metodologia cien#fica de análise bibliográ$ca com o intuito de evidenciar as t%cnicas de Phishing mais comuns e os métodos de conscientização mais eficazes. Uma vez levantados esses dados, partiu-se então para a de$nição da ferramenta a ser utilizada como "Phishing A) areness Tool", ferramenta esta capaz de prover recursos de simulação de Phishing, engajamento do usuário, detecção automatizada, avaliação con#nua, além de propiciar, relatórios e métricas. Visando este cenário, a ferramenta escolhida foi a - ophish. Para galgar terreno e atingir o objetivo estabelecido, foi empregada uma pesquisa aplicada de caráter explorat"rio com abordagem qualitativa utilizando-se de uma metodologia cien#fica de análise experimental no desenvolvimento de simulação de Phishing na ferramenta - ophish, a qual foi utilizada em teste prático com determinado grupo de indivíduos. De posse dos referidos testes e após uma análise detalhada de seus resultados, foi possível gerar um módulo de feedback e treinamento para os usuários por meio de uma cartilha de conscientização de Phishing.

Palavras-chave: *Phising, Conscientização, Ferramenta, 2iscos, Gophish*

1 INTRODUÇÃO

A segurança cibernética é uma preocupaçã o crescente em organizações militares devido ao aumento de ataques de *phishing*. Segundo Cardoso e Nunes (2020), “o ataque de *phishing* é uma das formas mais comuns de engenharia social, visando roubar informações sensíveis”.

Isto posto, a finalidade desta pesquisa é propiciar a conscientização dos riscos e ameças referentes ao phishing dentro de determinada organização.

A evolução da tecnologia trouxe consigo diversos avanços no cotidiano de todos os indivíduos, entretanto, toda tecnologia, quando utilizada com más intenções, pode ser uma ferramenta extremamente perigosa. Dentre o vasto universo de mecanismos tecnológicos maliciosos, está o *phishing,* o qual se destaca como uma das ameaças mais insidiosas e amplamente disseminadas. Neste estudo, estará em voga a conscientização sobre *phishing*, suas estratégias e os impactos que essa prática tem na segurança das informações.

A conscientização sobre *phishing* é fundamental para proteger indivíduos e organizações contra esses ataques. Afinal, a primeira linha de defesa está nas mãos dos próprios usuários. Quando as pessoas compreendem as táticas empregadas por criminosos ficam alertas aos os sinais de *phishing*, a probabilidade de sucesso desses ataques diminui consideravelmente.

1.1 CONTE5TUALIZAÇÃO DO ESTUDO

O termo *phishing* é uma palavra derivada do inglês *“fishing”* (pesca) e reflete a ideia de lançar iscas *para* atrair vítimas desavisadas. Trata-se de uma técnica sofisticada em que atacantes se passam por entidades confiáveis (como bancos, empresas ou serviços online) para enganar usuários e obter informações sensíveis, como senhas, dados bancários e informações pessoais. Esses ataques ocorrem principalmente por meio de e-mails, mensagens de texto, redes sociais e inclusive clonados.

1.2 JUSTIFICATIVA

O presente estudo justifica-se frente à latente persistência de ataques *phishing*, representando assim uma possível ameaça presente para qualquer setor. Fato esse corroborado por Carvalho (2022):

> Dados do relatório *Strategic Securit6 Surve6* produzido pela *Dar0 2eading* apontam que, em 2021, 53% das organizações citaram o phishing como causa direta de incidentes de segurança.

Apesar do referido cenário, pouco há sobre a conscientização de tais ameaças e, visando preencher tal lacuna e entregar uma ferramenta clara e objetiva, este estudo produzirá uma cartilha pautada nos resultados de pesquisa bibliográfica combinada com uma pesquisa exploratória.

147DEFINIÇÃO DO PROBLEMA DE PESQUISA

Diante da crescente sofisticação dos ataques de *phishing* e da constante evolução das técnicas utilizadas por mentes mal-intencionadas, como é possível promover uma conscientização eficaz entre os usuários? Quais estratégias são mais adequadas para educar e proteger as pessoas contra essas ameaças? Como mostrar de maneira tangível os riscos dessa ameaça para o usuário?

1.4 OBJETI6OS DA PESQUISA

Este trabalho pretende: delimitar os principais atributos de uma ferramenta para testes de exposição ao *phishing*; investigar as estratégias de conscientização de phishing mais eficazes; avaliar o impacto dessas estratégias na segurança cibernética e propor diretrizes para a implementação de uma cartilha de conscientização e prevenção contra-ataques *phishing.*

1.5 ESTRUTURA DO CONTEÚDO ESCRITO

O presente estudo está organizado da seguinte forma:

1.5.1 INTRODUÇÃO

Definida pela contextualizaçto, justificativa, problema de pesquisa, relevância e objetivos.

1.5.2 DESENVOLVIMENTO

Breve apresentaçto da problemática na qual a pesquisa se insere e se propõe a entregar uma soluçto viável de mitigaçto.

1.5.2.1 REVISÃO DA LITERATURA

A partir da literatura revisada, trata das estratégias de conscientizaçto, técnicas de *phishing* mais latentes, definir os principais atributos de uma ferramenta para testes de exposiçto ao *phishing* e escolhê-la de fato, além de delimitar o ativo que será empregado para disponibilizaçto online do serviço da campanha.

1492.2 METODOLOGIA DE PESQUISA

Visa expor um determinado grupo a simulações de *phishing* de maneira controlada e assim poder analisar e explorar os resultados obtidos da experimentaçto.

Sendo assim, a pesquisa foi conduzida em duas fases: uma fase de pré-campanha, na qual foi avaliada a vulnerabilidade inicial dos participantes, e uma fase de pós-campanha, na qual foi medida a eficácia da campanha educativa. Foram utilizados questionários e simulações de ataques de *phishing* para coletar dados

1.5.247APRESENTAÇÃO E ANÁLISE DE DADOS

Análise crítica e interpretativa dos dados coletados durante a pesquisa exploratória a fim de obter reflexões sobre os impactos observados.

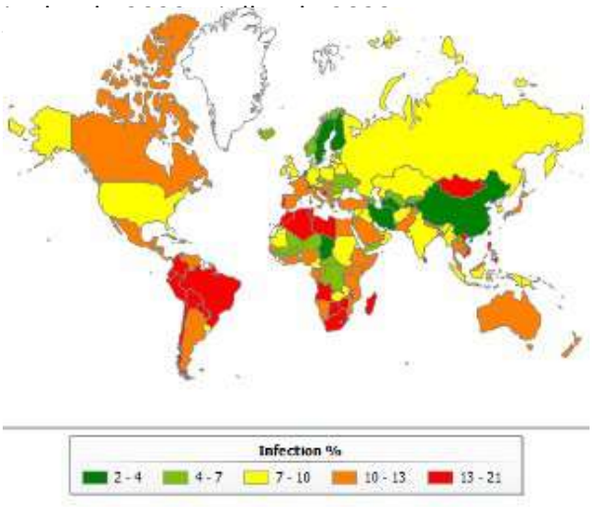
1.5.2.4 DISCUSSÃO DOS RESULTADOS

Síntese dos principais produtos obtidos com o estudo de modo a propiciar recomendações para a prática da confecçto da cartilha.

2 DESENVOLVIMENTO

A conscientização sobre phishing é uma componente essencial da segurança cibernética moderna. Com o aumento da sofisticaçto dos ataques, as organizações precisam adotar estratégias eficazes para educar seus funcionários e proteger seus dados.

Nos últimos anos, o Brasil tem registrado um aumento significativo nos casos de *phishing*, um t ipo de fraude eletrônica na qual criminosos t entam obter informações pessoais e financeiras das vítimas por meio de mensagens enganosas. De acordo com um relatório da Kaspersky (empresa de cibersegurança), houve um crescimento de significativo nas tentativas de *phishing* no Brasil entre



Fonte: kaspersky, 2023.

O aumento expressivo está associado à retomada das atividades econômicas pós-pandemia e ao uso de ferramentas de Inteligência Artificial para criar conteúdos fraudulentos de forma automatizada.

Não obstante, o Brasil lidera o *ranking* de países mais afetados por ataques de *phishing* na América Latina, com 134 milhões de tentativas de ataque registradas no período analisado. Os setores mais visados incluem o governo e o setor financeiro, além dos usuários comuns da internet.

A pandemia de COVID-19 também contribuiu para o aumento dos ataques de phishing, com criminosos aproveitando a desinformação e o medo generalizado para disseminar golpes relacionados a programas de auxílio social e outras falsas promessas. Em 2021, por exemplo, houve um aumento de 41% nos ataques de *phishing* em comparação ao ano anterior.

FIGURA 2: Tentativas de Phishing na Pandemia

Fonte: Kaspersky Lab, 2020.

As informações obtidas evidenciam a relevância de implementar medidas de segurança robustas e de promover a conscientização dos usuários para a identificação e prevenção de tentativas de *phishing*. A educação digital e o uso de tecnologias de proteção são fundamentais para mitigar os riscos associados a esse tipo de ameaça.

2.1 REVISÃO DA LITERATURA

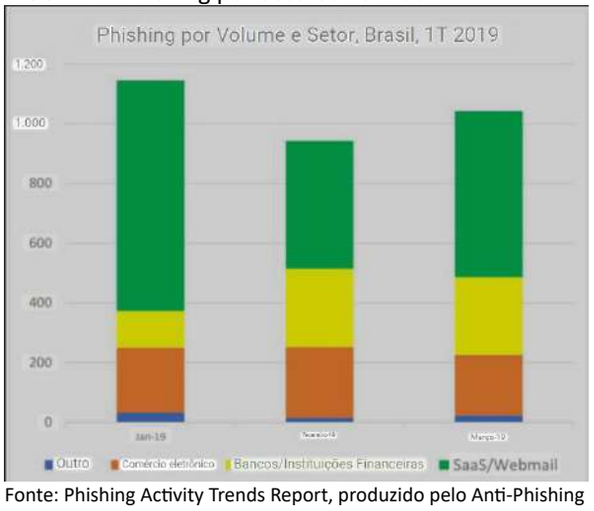
Inicialmente, é necessário definir de maneira clara o que é e como funciona um ataque *phishing.* Segundo *7 alwareb6tes* (2024):

> O *phishing* é uma forma de crime cibernético em que os criminosos tentam obter informações confidenciais por e-mail com links fraudulentos, solicitando que você preencha um formulário com suas informações de identificação pessoal. Em seguida, eles podem usar essas informações para obter suas credenciais on-line para perfis de mídia social, contas bancárias e muito mais.
>
> O *phishing* envolve o envio de mensagens falsas que parecem reais e urgentes, como e-mails, chamadas telefônicas ou mensagens de texto, para enganar as pessoas a compartilharem informações confidenciais. Os golpistas se passam por entidades legítimas, como bancos, e criam um senso de urgência para persuadir as vítimas a inserir dados

pessoais em sites falsos. Isso pode levar ao roubo de ident idade e a perdas financeiras.

Programas de treinamento contínuo ajudam os elementos de uma organização a reconhecer e responder adequadamente a tentativas de phishing, portanto, realizar simulações periódicas pode ajudar a identificar vulnerabilidades e reforçar o treinamento. Em vez de punir os indivíduos que caem em simulações, uma abordagem positiva que incentiva a identificação correta e recompensa os esforços pode ser mais eficaz. Afinal, segundo Noonan (2024), "O *Phishing* é um problema grave para empresas de todas dimensões e de todos os setores", situação essa demonstrada a seguir com gráfico que demonstra uma crescente dos casos no Brasil

FIGURA 7#Phishing por Setores no Brasil



Fonte: Phishing Activity Trends Report, produzido pelo Anti-Phishing Working Group (APWG).

Sendo assim, vale ressaltar a seguinte observação de Probst (2024):

> […] Além disso, novas tecnologias utilizadas por agentes maliciosos para além de sua finalidade legítima, como a inteligência artificial, aumentam o potencial danoso desta técnica criminosa. Por isto, implementar campanhas *anti-phishing* não é apenas uma medida preventiva, mas uma estratégia essencial de segurança.

Atualmente, as técnicas de phishing mais sofisticadas incluem o uso de IA, onde cibercriminosos criam mensagens personalizadas para enganar até os usuários mais experientes. O *vishing* utiliza chamadas telefônicas para obter dados pessoais, enquanto o *smishing* envia mensagens de texto enganosas. No *phishing* de aplicativos, criminosos desenvolvem apps falsos que imitam os legítimos. O voicemail *phishing* usa mensagens de voz falsas, e a engenharia social manipula psicologicamente as vítimas para obter informações confidenciais. Essas técnicas estão se tornando mais complexas, exigindo maior vigilância e medidas de segurança robustas de todos.

Desse modo, observa-se que o *phishing* constitui uma técnica de engenharia social empregada por agentes mal-intencionados com o intuito de ludibriar usuários e obter informações sensíveis, tais como senhas e dados bancários. Uma das maneiras de implementação dessa técnica é a utilização do - *ophish*, uma valiosa ferramenta de código aberto que possibilita a criação e execução de campanhas de *phishing* de maneira simplificada. Conforme estudos recentes, o - *ophish* é amplamente utilizado tanto por pesquisadores de segurança quanto por criminosos, devido à sua facilidade de uso e eficácia (SILVA, 2023).

A estrutura de uma campanha de *phishing* utilizando o - *ophish* geralmente envolve múltiplas etapas. Normalmente, o atacante começa por configurar um servidor de *phishing*, onde são hospedadas páginas fraudulentas que imitam sites legítimos. Subsequentemente, são elaborados e-mails de *phishing* que contêm links para essas páginas fraudulentas. Esses arquivos são enviados a um elevado número de vítimas potenciais. Quando uma vítima clica no link e insere suas informações na página fraudulenta, esses dados são capturados pelo servidor de *phishing* (SOUZA, 2022).

Estudos indicam que as técnicas de engenharia social presentes nos e-mails de *phishing* aumenta significativamente a taxa de sucesso das campanhas. Isso é realizado através da coleta de informações sobre as vítimas, como nomes e cargos, para tornar os e-mails mais convincentes. Ademais, a utilização de técnicas de *spoofing* de e-mail, onde o endereço do remetente é falsificado para parecer que o e-mail foi enviado por uma

fonte confiável, também é comum (FERREIRA, 2021).

A eficácia do - *ophish* e de outras ferramentas de *phishing* ressalta a importância de medidas de segurança robustas, como a educação dos usuários e a implementação de autenticação multifator. Conforme apontado por especialistas, a conscientização sobre as técnicas de *phishing* e a adoção de boas práticas de segurança são essenciais para mitigar os riscos associados a essas ameaças (COSTA, 2020).

O - *ophish*, uma ferramenta de *phishing* de código aberto e gratuita, o qual foi concebido para atender às necessidades de empresas e testadores de penetração, proporcionando um ambiente robusto para a criação de campanhas de simulação de *phishing*. A escolha do - *ophish* como ferramenta de conscientização sobre os perigos dos golpes cibernéticos é justificada por diversos fatores positivos, conforme delineado em seu manual.

FIGURA 4: - *ophish,* código aberto

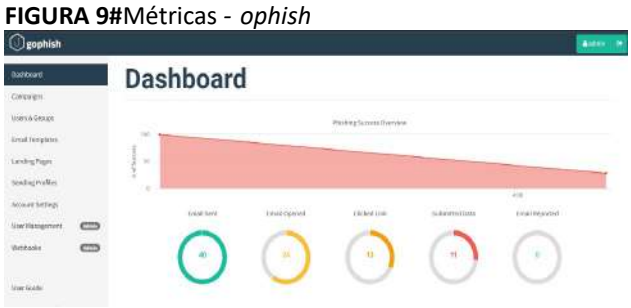
Fonte: Cyberpunk (2024).

Primeiramente, o - *ophish* destaca-se pela sua facilidade de uso e interface intuitiva, permitindo que usuários que detenham conhecimentos técnicos limitados possam configurar e executar campanhas de *phishing* de maneira eficaz. Essa acessibilidade é crucial para a implementação de programas de conscientização em larga escala, onde a simplicidade e a eficiência são essenciais (GOPHISH, 2024).

Além disso, o - *ophish* oferece flexibilidade na personalização das campanhas, permitindo a criação de e-mails e páginas de *phishing* que imitam com precisão os sites legítimos. Essa capacidade de personalização é fundamental para simular cenários realistas e, assim, aumentar a eficácia do treinamento dos usuários. A personalização também facilita a adaptação das campanhas às necessidades específicas de diferentes organizações, tornando o treinamento mais relevante e impactante (GOPHISH, 2024).

Outro ponto positivo do - *ophish* é a capacidade de monitoramento e análise detalhada dos resultados das campanhas. A ferramenta fornece métricas abrangentes sobre o comportamento dos usuários, como taxas de abertura de e-mails, cliques em links e submissão de dados. Essas informações são valiosas para identificar vulnerabilidades e ajustar as estratégias de segurança conforme necessário. A análise detalhada permite uma avaliação precisa da eficácia das campanhas de conscientização e do nível de preparação dos usuários contra-ataques de *phishing* (GOPHISH, 2024).

FIGURA 9#Métricas - *ophish*



Fonte: Os autores.

Por fim, o - *ophish* é uma ferramenta altamente escalável, capaz de suportar campanhas de *phishing* em organizações de qualquer tamanho. Sua arquitetura de código aberto permite que seja adaptado e expandido conforme as necessidades específicas de cada organização, garantindo que a ferramenta possa crescer junto com a empresa e suas demandas de segurança (GOPHISH, 2024).

Em suma, a escolha do - *ophish* para a conscientização sobre os perigos dos golpes cibernéticos é amplamente justificada por sua facilidade de uso, flexibilidade, capacidade de monitoramento e análise, e escalabilidade. Essas características fazem do - *ophish* uma ferramenta poderosa e eficaz para educar os usuários e fortalecer a postura de segurança de determinada organização frente aos latentes ataques de *phishing* do mundo atual.

Uma vez definida a ferramenta, é necessário partir à aplicabilidade da campanha de *phishing*, portanto, é imprescindível o emprego de um meio de disponibilização online da *landing page* empregada através do - *ophish,* de modo que o participante que tenha recebido o link em seu e-mail consiga acessar a partir de qualquer link de internet. Com base nisso, entra em voga a hospedagem na nuvem.

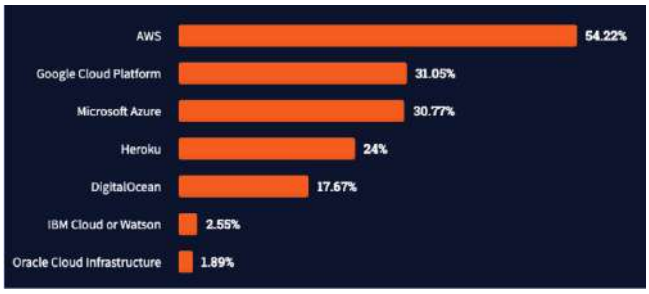
A hospedagem de serviços na nuvem tem se mostrado uma opção cada vez mais atrativa para empresas de todos os tamanhos devido à combinação de segurança robusta e facilidade de uso. A computação em nuvem permite que dados e aplicativos sejam armazenados em servidores remotos, acessíveis via internet, eliminando a necessidade de investimento em infraestrutura física. Entre as opções mais populares de serviços em nuvem estão Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP). A AWS, especificamente, destaca-se por sua escalabilidade e flexibilidade, permitindo que recursos sejam ajustados conforme a demanda do usuário. Além disso, a AWS oferece medidas de segurança rigorosas, como criptografia de dados e controle de acesso baseado em políticas. O plano gratuito da AWS é um grande atrativo, proporcionando acesso a uma variedade de serviços sem custos iniciais, o que é ideal para pequenas empresas e startups que desejam testar suas aplicações ou campanhas com um orçamento limitado (Amazon Web Services, 2024; Microsoft Azure, 2024; Google Cloud Platform, 2024).

TABELA 1: Comparação entre Serviços de Nuvem

Serviço	Flexibilidade	Segurança	Preço	Suporte
Amazon Web Services (AWS)	Alta	Alta	Variável	Excelente
Microsoft Azure	Alta	Alta	Variável	Bom
Google Cloud Platform (GCP)	Alta	Alta	Variável	Bom
Hostinger	! édia	! édia	con(mic	Regular
SiteGround	! édia	! édia	con(mic	Bom

Fonte: Elaborada pelos autores com base em Amazon Web Services (2024), Microsoft Azure (2024), Google Cloud Platform (2024), Hostinger (2024) e SiteGround (2024).

FIGURA <#Plataforma de nuvem mais usada



Fonte: Zup (2021).

O uso de AWS para uma campanha de phishing, por exemplo, oferece vantagens significativas. Os recursos gratuitos permitem a criação de ambientes de teste seguros e escaláveis, sem a necessidade de gastos adicionais. A flexibilidade da AWS facilita a personalização e o ajuste dos recursos para atender às necessidades específicas da campanha. Outro ponto positivo é a segurança oferecida pela AWS, garantindo que os dados estejam protegidos contra acessos não autorizados. A documentação extensa e o suporte técnico de qualidade também são fatores que facilitam a implementação e o gerenciamento dos serviços na nuvem (Amazon Web Services, 2024; Hostinger, 2024; SiteGround, 2024).

TABELA 2: Vantagens do AWS

Vantagem	Descrição
Custo	Plano gratuito disponível para novos usuários
Facilidade de uso	nterface intuitiva e documentação abrangente
Escalabilidade	Alta escalabilidade para ajustar recursos
Segurança	Medidas de segurança robustas, incluindo criptografia
Suporte técnico	Suporte 24/7 e vasta comunidade de usuários
Ferramentas adicionais	Integraç, o com diversos serviços e APIs

Fonte: Elaborada pelos autores com base em Amazon Web Services (2024)5

Dessa forma, a AWS se apresenta como uma escolha sólida devido à sua combinação de escalabilidade, flexibilidade, segurança e custo-benefício. A disponibilidade de um plano gratuito torna a AWS uma opção acessível para iniciar projetos e campanhas sem grandes investimentos financeiros, ao mesmo tempo em que aproveita uma infraestrutura

de alta qualidade e suporte técnico especializado (Amazon Web Services, 2024).

2.2 MÉTODOS DE PESQUISA

Este estudo foi conduzido com o objetivo de produzir uma eficaz campanha de conscientização sobre *phishing* utilizando a ferramenta - *ophish*. O desenho da pesquisa seguiu um modelo experimental, onde os participantes foram expostos a simulações de ataques de *phishing* e posteriormente avaliados quanto à sua capacidade de identificar e evitar tais ataques. Sendo possível assim obter uma cartilha completa direcionada especificamente à condução e reprodução desta pesquisa em qualquer ambiente organizacional controlado.

A população-alvo deste estudo consistiu-se de alunos do curso de Oficial de Comunicações, curso de Gestão de Sistemas Táticos de Comando e Controle e curso de Telegrafista, cursos estes ministrados na Escola de Comunicações (ESCOM). A amostra foi composta por 37 alunos de diferentes especializações e níveis de familiaridade com o ambiente digital garantindo uma representação adequada de diferentes padrões de comportamento quando expostos à simulação de *phishing*.

2.2.1 PREPARAÇÃO DA CAMPANHA DE PHISHING

A fim de obter os e-mails dos destinatários pertencentes ao grupo foco do estudo, foi necessário fazer um levantamento junto ao integrante mais antigo do grupo, todavia, em um ambiente organizacional, é possível obter essa informação facilmente por meio da existência natural do cadastro dos integrantes.

Na sequência, utilizando a ferramenta - *ophish*, foi criada uma campanha de *phishing* simulada. O *template* do e-mail e da própria *landing page* da campanha foram construídos com base em técnicas de engenharia social atinentes ao referido grupo.

Os e-mails foram projetados para imitar comunicações legítimas da escola, incluindo logotipos e estilos de escrita comuns. O código fonte do *template* empregado no e-mail foi confeccionado pelos autores com auxílio de IA. O código fonte do *template* da página da campanha foi obtido diretamente da página do *"Captive Portal4* sendo necessárias apenas algumas modificações para o emprego.

2.2.2 EXECUÇÃO DA CAMPANHA

Os e-mails de *phishing* foram enviados aos participantes e estes, por sua vez, tiveram uma janela de aproximadamente cinco dias para travar contato ou nto com o e-mail em sua caixa de entrada. Cada participante recebeu um e-mail de *phishing*, sem aviso prévio, às cegas, para simular um cenário realista.

Uma vez recebido o e-mail, o indivíduo já está inserido no ambiente de pesquisa podendo ele abri-lo ou nto, clicar no link e até mesmo submeter dados solicitados, denotando claramente crença na veracidade da origem das solicitações.

Após a conclusto da campanha, é iniciada uma nova campanha a qual encaminha um e-mail informativo aos participantes sobre sua participaçto em uma campanha de conscientizaçto de *phishing,* além de solicitar o preenchimento de um questionário referente à experiência acompanhado de um link contendo um artigo sobre a tema em foco.

Foi confeccionado também um *script* em *p6thon,* o qual é capaz de coletar os dados resultantes de uma campanha do - *ophish* e ordená-los de maneira automática em uma tabela por participante. Essa tabela é remetida anexa ao e-mail de *feedback* da campanha.

2.247COLETA DE DADOS

A ferramenta - *ophish* registrou as interações dos participantes com os e-mails de *phishing*, incluindo se abriram o e-mail, clicaram em links ou forneceram informações sensíveis.

Após a campanha, foi enviado um questionário aos participant es para avaliar seu nível de conscientizaçto sobre *phishing* antes e depois da campanha.

2.2.4 TÉCNICAS DE ANÁLISE

2.2.4.1 ANÁLISE 8 UANTITATIVA

Os dados coletados pela ferramenta - *ophish* foram analisados para determinar a axa de sucesso dos e-mails de *phishing* (porcentagem de e-mails abertos, links clicados e informações fornecidas).

As respostas ao questionário foram analisadas para medir mudanças no nível de conscientizaçto dos participantes.

2.2.4.2 ANÁLISE 8 UALITATIVA

Comentários abertos dos participantes foram analisados para identificar percepções e sentimentos em relaçto à campanha de *phishing* e à conscientizaçto sobre segurança.

2.2.4.9 REPRODUTIBILIDADE DO ESTUDO

Para garantir que outros pesquisadores possam reproduzir este estudo, apresentar-se-á de maneira objetiva os passos necessários para sua execuçto. No entanto, é importante destacar que o objetivo principal desta pesquisa foi a elaboraçto de uma cartilha detalhada, que descreve todas as táticas, técnicas e procedimentos empregados na execuçto do estudo. Para uma compreensto mais aprofundada, é imprescindível a leitura da cartilha, que pode ser encontrada no Apêndice A – Instalaçto, Configuraçto e Operaçto do Sistema Empregado. Esta cartilha aborda os seguintes processos: implementaçto e configuraçto da máquina virtual no sistema de computaçto em nuvem (AWS); instalaçto e configuraçto da ferramenta - *ophish*; implementaçto dos templates de e-mail e *landing page* utilizados; *configuração* do método de envio SMTP; execuçto da campanha; acompanhamento da campanha; análise dos dados; aplicaçto do questionário e coleta de *feedback*.

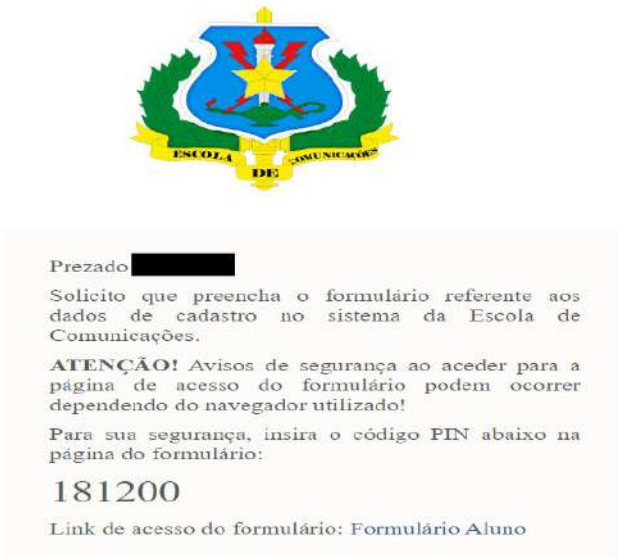
2.3 APRESENTAÇÃO E ANÁLISE DE DADOS

A coleta de dados nesta pesquisa se baseou nos resultados obtidos através da campanha hospedada pelo sistema - *ophish*. Tal coleta dividiu-se em dois momentos principais, os quais foram: Campanha Inicial de Conscientizaçto sobre p*hishing* (às cegas) e módulo de *feedback* pós campanha.

2.4 CAMPANHA INICIAL

Foram disparados e-mails para os 37 alunos participantes da pesquisa. Esse e-mail continha um PIN e descrevia a necessidade de fornecê-lo na subsequente página de redirecionamento para um formulário de atualizaçto cadastral para alunos da EsCom.

FIGURA !# **emplate* e-mail campanha inicial



Fonte: Os autores.

O intuito de utilizar a sistemática do código PIN para redirecionamento do acesso ao formulário é causar uma falsa sensação de segurança no participante de modo a legitimar o acesso ao formulário subsequente.

FIGURA =# **emplate* página campanha inicial

Fonte: Os autores.

Uma vez passado pela página de redirecionamento, o participante chega a um formulário - *oogle !orms*, este já não mais hospedado pelo sistema - *ophish,* mas sim no próprio sistema - *oogle*. A essa altura, pressupõe-se que o participante acredita na legitimidade da solicitação e está disposto a fornecer os dados, sejam estes quais forem. Ainda assim, os dados requeridos foram triviais, haja vista o objetivo desta pesquisa ser meramente educacional.

FIGURA >#Formulário campanha inicial

Fonte: Os autores.

A campanha esteve ativa durante aproximadamente 5 (cinco) dias e os dados obtidos podem ser visualizados de maneira geral através do próprio *dashboard* do sistema:

FIGURA 10: *Dashboard Gophish* campanha inicial

Fonte: Os autores.

Com o intuito de otimizar a visualização dos resultados da campanha bem como remeter tais resultados de maneira clara e objetiva para os participantes, foi empregado um *script* em *p6thon* o qual entrega uma tabela contendo os resultados de maneira organizada e objetiva. A íntegra e descrição desse *script* encontrar-se-á no anexo A.9.1 do apêndice A referente à cartilha de conscientização produto dessa pesquisa:

TABELA 7#Tabela de resultados pelo *script*

status	ip	email	Grad	Sobrenome
Enviou Dados	132.255.30.164	araujo2bec@gmail.com	Ten	Araujo
Enviou Dados	13.64.229.66	leonardoneves48@hotmail.com	Ten	Neves
Enviou Dados	177.8.80.142	rocha.matheussilva@eb.mil.br	Ten	Rocha
Enviou Dados	177.8.80.142	pedrohcdwattimo@gmail.com	Ten	Wattimo
Email Enviado	-	dasilva.lopes@eb.mil.br	Ten	Jonathas
Email Opened	66.249.88.198	mbcd08@gmail.com	Ten	Brandalize
Clicou no link	189.6.31.40	capbrandao2011@gmail.com	Cap	Brandão
Email Enviado	-	wanderleysd@gmail.com	Cap	Wanderley
Email Opened	66.249.91.131	marcoshotsizzle12@gmail.com	Sgt	Marcos Resende
Enviou Dados	187.73.144.228	philipzim02@gmail.com	Sgt	Philip
Enviou Dados	177.10.57.229	alencar.work3@gmail.com	Sgt	Lucas Alves
Email Enviado	-	crlerbes@gmail.com	Sgt	Erbes
Enviou Dados	187.43.181.184	sgtricciele@gmail.com	Sgt	Ricciele
Email Opened	66.249.91.131	israelchaga@gmail.com	Sgt	Israel Chagas
Email Opened	66.249.83.83	leeo7kennedy@gmail.com	Sgt	Kennedy
Email Opened	66.102.8.131	caiodesouza242@gmail.com	Sgt	Caio
Email Enviado	-	vccostab0@gmail.com	Sgt	Victor Costa
Enviou Dados	66.249.88.199	luanepcn05@gmail.com	Sgt	Luan Martins
Email Opened	66.249.91.131	vasconcelosgn@gmail.com	Ten	Vasconcelos
Email Opened	66.249.91.131	cad5043pedrocosta@gmail.com	Ten	Pedro Chaves
Email Opened	177.8.80.142	wesley.tri@hotmail.com	Ten	Wesley
Clicou no link	189.112.10.6	victorhugovelasque@gmail.com	Ten	Velasque
Email Enviado	-	olimpio8179@hotmail.com	Ten	Olimpio
Enviou Dados	191.58.137.0	vitorpaladi@hotmail.com	Ten	Paladini
Enviou Dados	191.56.49.113	robertomarques94@gmail.com	Ten	Roberto Marques
Email Opened	66.102.8.130	willianv.vduarte@gmail.com	Ten	Victor Ventura
Email Enviado	-	pedrocestarioli@hotmail.com	Ten	Cestarioli
Enviou Dados	177.8.80.142	guicabralg@gmail.com	Ten	Gomes
Email Opened	66.249.91.133	bergf2911@gmail.com	Ten	Berg
Email Enviado	-	wendellgomes.pereira@eb.mil.br	Ten	Wendell Gomes
Enviou Dados	177.8.80.142	vitor.villela@eb.mil.br	Ten	Vilela
Email Enviado	-	david_sumaio@outlook.com	Ten	Sumaio
Enviou Dados	177.8.80.142	sella.matheus@eb.mil.br	Ten	Sella
Email Enviado	-	thyago3551@gmail.com	Ten	Thyago Henrique
Email Opened	66.249.88.198	cirojosepadua@gmail.com	Ten	Padua
Email Enviado	-	pauloc.dealmeida89@gmail.com	Ten	Custódio
Enviou Dados	177.8.80.142	calmeida.santos@eb.mil.br	Ten	C Almeida
Enviou Dados	177.8.80.142	erick.schlotefeldt@eb.mil.br	Ten	Schlotefeldt

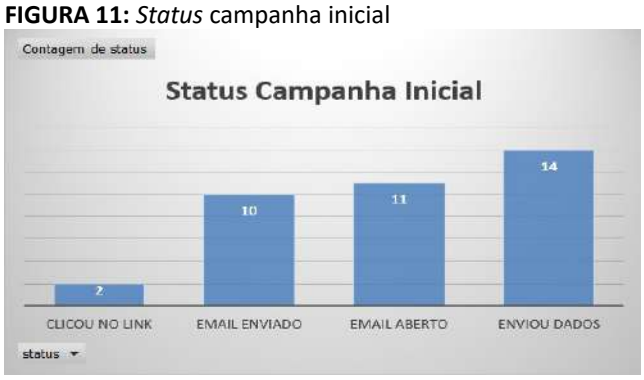
Fonte: Os autores.

Agora, com os dados resultantes da campanha aplicada, é possível observar que o grupo participante é heterogêneo. Em um universo de 37 participantes, todos com diferentes níveis de conhecimento e contato com ameaças cibernéticas, como *phishing*, foi possível subdividi-los em quatro subgrupos: 26% não abriram o e-mail; 28% abriram o e-mail; 5% abriram o e-mail e clicaram no link; e 44% clicaram no link e submeteram os dados solicitados.

Esses resultados revelam diferentes reações dos participantes ao interagirem com a campanha, lembrando que o contato foi às cegas, sem influências externas. O fato de alguns indivíduos não abrirem o e-mail pode indicar desatenção ou desconfiança na procedência do e-mail. Em ambos os casos, isso é significativo, pois um possível atacante poderia tentar múltiplas vezes até capturar a atenção da vítima.

Nos demais subgrupos, a vulnerabilidade em relação às ameaças *phishing* se torna evidente. Apenas abrir o e-mail já pode infectar a máquina da vítima, dependendo do conteúdo malicioso. Portanto, a conscientização desses subgrupos é crucial para que eles possam identificar sinais suspeitos e evitar ao máximo a exposição a essas ameaças.

FIGURA 11: *Status* campanha inicial



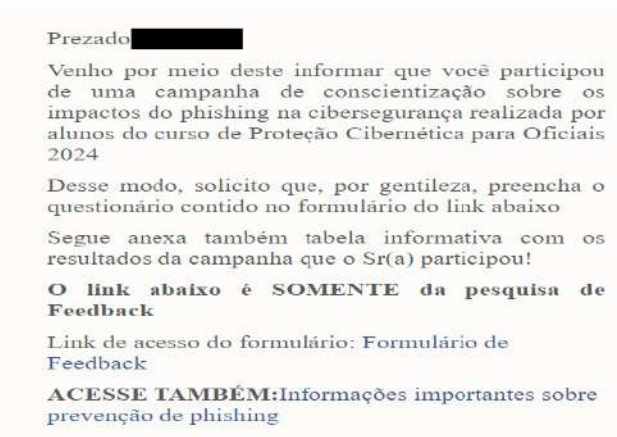
Fonte: Os autores.

247.2 MÓDULO DE FEEDBACK

Uma vez concluída a campanha inicial, é chegado o momento de promover o *feedback* aos participantes a fim de implantar de fato a ideia de conscientização sobre a ameaça *phishing,* além de colher dados referentes a experiência de participação e contato prévio com *phishing*. Tais dados serão de grande valia para o melhoramento de campanhas futuras e retificação do aprendizado.

O módulo consiste em um e-mail disparado através do próprio - *ophish* para todos os participantes da campanha inicial, contendo: um informativo sobre sua participação na campanha com a tabela de resultados anexa, um link para um material online sobre conscientização contra *phishing* e solicita a resposta a breves 12 (doze) questões sobre as experiências prévias e posteriores à participação na campanha. O questionário encontra-se pormenorizado no apêndice referente à cartilha de conscientização de *phishing*.

FIGURA 12: *Template* e-mail *feedback*



Prezado [redacted]

Venho por meio deste informar que você participou de uma campanha de conscientização sobre os impactos do phishing na cibersegurança realizada por alunos do curso de Proteção Cibernética para Oficiais 2024

Desse modo, solicito que, por gentileza, preencha o questionário contido no formulário do link abaixo

Segue anexa também tabela informativa com os resultados da campanha que o Sr(a) participou!

O link abaixo é SOMENTE da pesquisa de Feedback

Link de acesso do formulário: Formulário de Feedback

ACESSE TAMBÉM: Informações importantes sobre prevenção de phishing

Fonte: Os autores.

2.4 DISCUSSÃO DOS RESULTADOS

Os resultados obtidos pela campanha de conscientização sobre *phishing* indicam uma variedade de respostas e níveis de vulnerabilidade entre os 37 participantes. Esse comportamento heterogêneo destaca a complexidade em lidar com ameaças cibernéticas e a necessidade de estratégias adaptativas de conscientização.

Primeiramente, a constatação de que 26% dos participantes não abriram o e-mail de *phishing* pode ser interpretada de duas formas: desatenção ou desconfiança. A desatenção sugere que campanhas de *phishing* repetidas podem eventualmente capturar a atenção dessas pessoas. Por outro lado, a desconfiança é um sinal positivo de que algumas pessoas estão adotando uma postura cautelosa, essencial para a segurança cibernética.

Para os 28% que abriram o e-mail, mas não clicaram nos *links*, é evidente que há um grau de curiosidade ou necessidade de verificar o conteúdo. No entanto, este grupo ainda mostra uma vulnerabilidade significativa, pois o simples ato de abrir o e-mail pode expor o usuário a ameaças, dependendo do conteúdo malicioso inserido.

A porcentagem de participantes que clicaram no link (5%) e, mais alarmante, aqueles que submeteram dados (44%), expõe

uma séria falha na capacidade de identificar e evitar tentativas de *phishing*. Esses indivíduos sto os mais suscetíveis a ataques e reforçam a urgência de intensificar os programas de conscientizaçto e treinamento.

As diferentes reações dos participantes, sem influências externas, enfatizam a necessidade de abordagens personalizadas na educaçto sobre segurança cibernética. A campanha demonstrou que, enquanto alguns indivíduos mostram um nível básico de precauçto, muitos ainda carecem de conhecimento e habilidades necessárias para se proteger adequadamente de ataques *phishing*.

Portanto, os resultados sublinham a importância de estratégias contínuas e dinâmicas de conscientizaçto, envolvendo simulações realistas, *feedback* imediato e atualizaçto constante das técnicas de defesa. Melhorar a conscientizaçto e a educaçto sobre *phishing* é crucial para reduzir as vulnerabilidades e fortalecer a postura de segurança cibernética dos indivíduos.

CONCLUSÃO

Esta pesquisa destacou a importância da conscientizaçto sobre ameaças de *phishing*, especialmente no ambiente organizacional militar, onde a segurança cibernética é essencial. Ao implementar uma ferramenta de simulaçto de *phishing*, como o - *ophish*, foi possível avaliar o nível de vulnerabilidade dos usuários e estruturar uma resposta educacional adaptada às necessidades identificadas. A pesquisa nto apenas testou o comportamento dos usuários, mas também desenvolveu um módulo de *feedback* e treinamento que oferece aos participantes os recursos necessários para melhorar sua capacidade de identificar e evitar ataques de *phishing* no futuro.

Os resultados da campanha mostraram a diversidade de respostas entre os participantes, que variaram desde aqueles que nto abriram o e-mail até os que submeteram dados, refletindo graus variados de conscientizaçto e vulnerabilidade em relaçto às ameaças de *phishing*. Esses resultados demonstram a necessidade de abordagens personalizadas e contínuas de conscientização, reforçando que a educação em segurança cibernética deve ser um processo constante e adaptável. A abordagem prática da pesquisa, através do uso do - *ophish*, permitiu aos participantes vivenciarem um cenário simulado de ataque, proporcionando uma experiência de aprendizagem prática e significativa.

Para o Exército Brasileiro, as contribuições destas pesquisas são valiosas e podem ser aplicadas em várias áreas. Contra o *phishing*, a conscientização e o treinamento podem ser estendidos a grupos de usuários diversificados, abrangendo não só a seção de informática das Organizações Militares, mas também todas as áreas onde o acesso a informações sensíveis representa um ponto crítico de segurança. A implementação de campanhas regulares de conscientização, com simulações de *phishing* e relatórios de desempenho, pode fortalecer a postura de segurança organizacional e reduzir as vulnerabilidades frente a ataques cibernéticos. Essa prática, quando amplamente adotada, promove uma cultura de segurança digital, que se torna um ativo estratégico, elevando o nível de proteção em todos os níveis da instituição.

É imprescindível integrar métodos de conscientização e treinamento que considerem aspectos psicológicos e culturais dos usuários, além de práticas contínuas para fortalecer a retenção de conhecimento. Campanhas que incluam simulações técnicas e abordagens interativas podem sensibilizar mais eficazmente os participantes, tornando-os mais atentos. A aplicação de métodos variados e de longo prazo contribui para uma postura sólida frente a ameaças, que evoluem constantemente e demandam vigilância permanente, afinal, tais ameças estão em constante evolução, logo é cada vez mais latente a continuidade de conscientização.

Em síntese, a pesquisa conseguiu responder à questão proposta, que visava entender como promover a conscientização efetiva sobre *phishing* em um ambiente organizacional. A aplicação do - *ophish* e o

desenvolvimento de uma cartilha educacional constituem um modelo replicável, adaptável a diferentes contextos dentro do Exército Brasileiro e de outras organizações. A eficácia do treinamento foi comprovada pelos resultados, que mostraram uma melhora no entendimento e na precaução dos usuários em relação aos ataques de *phishing*. Este estudo reforça a importância de investir em campanhas de conscientização cibernética, que devem ser contínuas e aprimoradas para acompanhar a evolução das ameaças digitais. Dessa forma, conclui-se o ciclo argumentativo proposto desde a introdução, reafirmando a necessidade de uma abordagem proativa para a educação em segurança digital e destacando o valor de uma postura de vigilância constante.

741 RESULTADOS

A campanha de simulação de *phishing* realizada com o uso da ferramenta - *ophish* proporcionou *insights* valiosos sobre o comportamento e o nível de conscientização dos usuários em relação às ameaças de *phishing*. Os resultados mostraram uma variedade de respostas dos participantes, desde aqueles que evitaram interagir com o e-mail suspeito até os que chegaram a submeter dados pessoais. Esses diferentes graus de vulnerabilidade destacam que, apesar de haver um nível geral de conscientização, muitos usuários ainda possuem lacunas de conhecimento que podem comprometer a segurança organizacional. A análise detalhada dos resultados permitiu desenvolver um módulo de *feedback* e treinamento específico, que se mostrou eficaz em melhorar a capacidade dos usuários de identificar e evitar futuros ataques de *phishing*.

7.2 IMPLICAÇÕES PR; TICAS E TEÓRICAS

As implicações práticas deste estudo são significativas para o contexto militar, onde a segurança cibernética é crucial. A aplicação da ferramenta Gophish demonstrou ser uma abordagem prática para testar vulnerabilidades e fornecer um treinamento de conscientização em segurança digital. Em termos práticos, a pesquisa sugere que campanhas de simulação de *phishing* e treinamentos regulares podem reduzir as vulnerabilidades institucionais e reforçar a cultura de segurança digital no Exército Brasileiro. Teoricamente, o estudo contribui para o campo da conscientização em cibersegurança ao demonstrar que uma abordagem prática e personalizada pode ser mais eficaz do que métodos tradicionais de conscientização. Além disso, destaca-se a importância de uma metodologia adaptável que seja capaz de evoluir de acordo com as ameaças cibernéticas em constante mudança.

743 LIMITAÇÕES E CONSIDERAÇÕES

Embora a pesquisa tenha gerado resultados importantes, algumas limitações devem ser consideradas. Primeiramente, o estudo foi aplicado a um grupo específico de usuários, o que limita a generalização dos resultados para outros grupos ou setores. Além disso, o tempo de exposição dos participantes à campanha de conscientização foi relativamente curto, o que pode ter influenciado a retenção de conhecimento a longo prazo. Outra limitação foi a dependência de uma única ferramenta (- *ophish*) para simulação de *phishing*, não abrangendo outras possíveis técnicas e abordagens de conscientização. Essas limitações sugerem a necessidade de cautela ao extrapolar os resultados e reforçam a importância de estudos complementares com amostras mais diversificadas e diferentes ferramentas de conscientização.

744 RECOMENDAÇÕES E DIREÇÕES FUTURAS

Para pesquisas futuras, recomenda-se expandir o tamanho e a diversidade da amostra, incluindo participantes de diferentes setores e níveis de acesso a informações sensíveis. Essa expansão permitirá uma avaliação mais ampla da eficácia das campanhas de conscientização de *phishing* em

diferentes contextos. Sugere-se também a realização de campanhas de conscientização de longo prazo, permitindo analisar a retenção de conhecimento e possíveis mudanças de comportamento em relação às ameaças de *phishing*. Além disso, futuras pesquisas poderiam explorar a eficácia de outras ferramentas e abordagens de conscientização, como treinamentos "gameficados" ou sistemas de alerta em tempo real. No contexto organizacional militar, recomenda-se a implementação de campanhas regulares e a criação de políticas institucionais que promovam a educação em cibersegurança como parte da rotina de trabalho dos usuários, fortalecendo uma postura proativa e adaptativa frente as ameaças digitais.

ABSTRACT

*This research aimed to raise awareness about the risks associated) ith Phishing threats and, for that purpose, sought to implement a tool capable of testing the exposure level of a specific group of users to this type of threat (n applied explorator6 study) ith a qualitative approach) as conducted, using a scientific methodology of bibliographic analysis to highlight the most common Phishing techniques and the most e8ective awareness methods (9er gathering this data, the next step) as to de$ne the tool to be used as a 'Phishing ( ) areness *ool,') hich) ould provide resources for Phishing simulation, user engagement, automated detection, continuous evaluation, as) ell as generating reports and metrics. In this context, the chosen tool) as - ophish. *o gain ground and achieve the established objective, an applied explorator6 study) ith a qualitative approach) as employed, using a scientific methodology of experimental analysis to develop a Phishing simulation on the - ophish tool,) hich) as then tested) ith a specific group of individuals. ; ased on these tests and after a detailed analysis of their results, it) as possible to create a feedback and training module for users through a Phishing awareness guide*

Keywords<*Phishing, A) areness, Tool, Risks, Gophish*

REFERÊNCIAS

ALVES, C. de S.; CAETANO, R. H. S. **PB)$B)-(Sc&+ - Am/)*- %* Militar# A EC,)D-,)& 2* um& T' ,-), & 2* Pr*E*-. F 2* A%aque$ 2* PB)$B)-(C - tr& M)1)a%*$**. O Comunicante, v. 12, n. 1, 2022.

AMAZON WEB SERVICES. **A+& G - H */ SerE),*$ IAH SJ**. 2024. Disponível em: <https://aws.amazon.com/>. Acesso em: 5 out. 2024.

CARDOSO, D. M. F.; NUNES, D. B. **Pr %*. F C - tr& A%aque$ 2* PB)$B)-(- Ex' r,)% Br&$)1i*** . O Comunicante, v. 10, n. 1, 2020.

CARVALHO, Leonardo. **PB)$B)-(# &)+ por%-,)& 2& C -$,)*- 0G&.F * 2 Tr*)-&+ *- % *+ $*(ur&-. & -& pr*E*-. F 2*$%& &+*&.&4** Disponível em: https://www.tempest.com.br/blog/phishing-a-importancia-da-conscientizacao-e-do-treinamento-em-seguranca-na-prevencao-desta-ameaca/#:~:text=O%20phishing%20continua%20representando%20uma,percentual%20era%20de%2051%25). Acesso em: 5 out. 2024.

COSTA, M. A. **T' ,-), &$ 2* phishing * + *2)2&$ 2* $*(ur&-. &4R*E)$%& 2* Se(ur&-. &2& InMr+ &.F** , v. 15, n. 3, p. 45-58, 2020.

CYBERPUNK. **Gophish: Ope-NSour, * PB)$B)-(T 1O)%4** Disponível em: <https://www.cyberpunk.rs/gophish-open-source-phishing-toolkit>. Acesso em: 5 out. 2024.

DEEPEN, Desai; HEGDE, Rohit. **Aum*- % 2 $ &%aque$ 2* phishing# r*1&6r) 2* phishing 2* 2024 2& Thr*&tLabG4** Disponível em: https://www.zscaler.com/br/blogs/security-research/phishing-attacks-rise-58-year-ai-threatlabz-2024-phishing-report?formCode=MG0AV3. Acesso em: 5 out. 2024.

DOS SANTOS, Demian. **C -$,)*- 0G&.F sobr* phishing * $*(ur&-. &# , + que M*quê-,)& tr*inar $ $*us Mncionár) $R4** Disponível em: https://www.diariodeti.com.br/conscientizacao-sobre-phishing-e-seguranca-com-que-frequencia-treinar-os-seus-funcionarios/. Acesso em: 5 out. 2024.

FALOURD, Guillaume. **STAC@O6 ERFLOH SUR6EY 2021# O 8UE APRENDEMOS COM A PESQUISA**. Disponível em: https://zup.com.br/blog/stack-overflow-survey-2021. Acesso em 07 out. 2024.

FERREIRA, L. R. **Spoofi- (2* *N- &)1* suas)+ plic&.T*$4** Jornal de Cibersegurança, v. 10, n. 2, p. 123-134, 2021.

GARTNER. **Gar%-*r For*, &$s H or12U)2* IT Spe-2)-(% Gr U 94V)- 20234** Disponível em: <https://www.gartner.com/en/newsroom/press-releases/2023-04-06-gartner-forecasts-worldwide-it-spending-to-grow-5-percent-in-2023>. Acesso em: 5 out. 2024.

GOOGLE CLOUD PLATFORM. **G (1* Cloud P1&N r+ IGCP)4** 2024. Disponível em: <https://cloud.google.com/>. Acesso em: 5 out. 2024.

GOPHISH. **Gophish User Guide**. 2024. Disponível em: https://docs.getgophish.com/user-guide. Acesso em: 20 set. 2024.

HARÁN, Juan Manuel. **C&+panhas 2* phishing**

, - 0nuam apr*$*- %&-2 , r*$,)+ *- % - Br&$)14 H *Liv*Se, ur)%X 03 set. 2019. Disponível em: https://www.welivesecurity.com/br/2019/09/03/campanhas-de-phishing-continuam-apresentando-crescimento-no-brasil/. Acesso em: 26 set. 2024.

HOSTINGER. **Hos0- (*r4** 2024. Disponível em: <https://www.hostinger.com.br/>. Acesso em: 5 out. 2024.

KASPERSKY. **Panor&+& 2* A+ *&.&$ 2023**. Disponível em: https://www.kaspersky.com.br/blog/panorama-de-ciberameacas-2023/21631/. Acesso em: 2 out. 2024.

KASPERSKY. **PB)$B)-(por H B&tsApp *+ 2022**. Disponível em: https://www.kaspersky.com.br/blog/phishing-whatsapp-antiphishing-informacoes-pessoais-dados-financeiros/21113/. Acesso em: 2 out. 2024

MALWAREBYTES. **O que ' phishingR**. Disponível em: https://www.malwarebytes.com/pt-br/phishing. Acesso em: 5 out. 2024.

MICROSOFT AZURE. **M),r $ Z Azur***. 2024. Disponível em: <https://azure.microsoft.com/>. Acesso em: 5 out. 2024.

NOOLAN. **O que ' um& $)+ulaçF 2* phishingR** Disponível em: https://www.metacompliance.com/pt/blog/phishing-and-ransomware/what-is-a-phishing-simulation. Acesso em: 5 out. 2024.

PROBST. **Cultur& positiE& par& aum*- %ar & $*(ur&-.& ,)/*r-' 0, & , orpor&0E&** Disponível em: https://www.grantthornton.com.br/insights/artigos-e-publicacoes/campanha-anti-phishing-cultura-positiva-para-aumentar-a-securanca-cibernetica-corporativa/. Acesso em: 5 out. 2024.

ROOTSEC. **C)-, + *lhor*$ $)+ulador*$ 2* phishing**. Disponível em: https://rootsec.com.br/cinco-melhores-simuladores-de-phishing/. Acesso em: 6 out. 2024.

SILVA, J. P. GoPhish: **Um& Mrr&+*- %&2* , P2)(&/*r% par&, &+panhas 2* phishing**. Revista de Tecnologia da Informação, v. 22, n. 1, p. 78-89, 2023.

SITEGROUND. **Sit*Ground**. 2024. Disponível em: <https://www.siteground.com/>. Acesso em: 5 out. 2024.

SOFTWARE TESTING HELP. **Top 4 BEST Ngr O Alt*r-&0E*$ In 2024**: Review And Comparison. Disponível em: https://www.softwaretestinghelp.com/ngrok-alternatives/. Acesso em: 26 set. 2024.

SOUZA, A. B. **Estrutur& 2* , &+panhas 2* phishing**. Revista Brasileira de Segurança Digital, v. 18, n. 4, p. 67-79, 2022.

ANÁLISE DE TROUGHPUT DO RÁDIO HARRIS RF-7800M-MP PARA O MODO DE OPERAÇÃO ANW2C

Cap GUSTAVO **BRANDÃO** DE BARROS CORREIA
Cap **THYAGO HENRIQUE** ALMEIDA SIMÕES
Cap **WANDERLEY** SOARES DIAS
Pós-Graduandos, lato sensu, em Gestão de Sistemas Táticos Comando e Controle

Resumo: Este estudo analisa o *throughput* do rádio Harris RF-7800M-MP, operando no modo ANW2C, avaliando o impacto do aumento do número de rádios nós sobre a capacidade de transmissão em rede. Os testes foram realizados em cinco cenários com diferentes quantidades de rádios, variando de 2 a 30 nós, e configurados com uma potência de transmissão intermediária de 2 watts, a uma distância de 50m e em visada direta. Utilizou-se a frequência de 1430 MHz, com uma largura de banda de 5 MHz, atendendo à regulamentação de uso militar, com o objetivo de alcançar o *throughput* teórico máximo de 10 Mbps em condições ideais. A coleta de dados foi realizada pelo *software* iPerf3, com análise prática do *throughput* através de simulações que consideraram as limitações físicas dos dispositivos. Os resultados indicaram que o *throughput* diminui progressivamente com o aumento do número de rádios na rede, destacando a necessidade de planejamento adequado na configuração das redes de Comando e Controle (C2) em operações militares.

Palavras-chave: Throughput. Rádio Harris RF-7800M-MP. Modo ANW2C. Redes ad hoc. Comunicações táticas

1. INTRODUÇÃO

Nas operações militares modernas, a comunicação segura e adaptável é essencial para a coordenação e proteção das tropas. Em conflitos recentes, como a guerra entre Rússia e Ucrânia, as comunicações e a segurança cibernética têm se mostrado cruciais, especialmente com o uso intensivo de guerra eletrônica e guerra cibernética para comprometer redes adversárias. Esse contexto destaca a importância de sistemas de comunicações resilientes e seguras para apoiar operações militares (BBC, 2022; MICROSOFT, 2022; UNITED STATES ARMY, 2022).

Nesse cenário, os rádios táticos desempenham um papel fundamental, especialmente os sistemas *ad hoc*, que possuem a capacidade de formar redes descentralizadas, autoformadas, e autorrecuperáveis, que promovem a flexibilidade necessária ao dinâmismo das operações.

1.1 Contexto e Importância do Estudo

Em operações convencionais, a robustez e a adaptabilidade das comunicações são vitais. O rádio Harris RF-7800M-MP, utilizado pelo Exército

Brasileiro (EB), destaca-se por fornecer comunicações seguras e adequadas a ambientes de alta mobilidade, suportando formas de onda como ANW2C, FM, AM, QUICKLOOK, HAVEQUICK e TALON (HARRIS CORPORATION, 2014). Esse rádio permite a criação de redes *ad hoc*, garantindo comunicações contínuas, essenciais em cenários de combate.

O modo ANW2C possibilita que cada rádio funcione como um nó repetidor, ampliando o alcance e criando rotas alternativas para a rede. Desta forma, estabelece uma rede *ad hoc* que fornece resiliência e flexibilidade aos sistemas de Comando e Controle (C2). Este estudo analisa o impacto do aumento do número de rádios nós no *throughput* da rede, cujos dados são relevantes para subsidiar o planejamento e a otimização das redes de C2.

1.2 Objetivo e Hipótese

O objetivo deste estudo é quantificar o impacto do aumento no número de rádios Harris RF-7800M-MP operando no modo ANW2C, como nós, sobre o *throughput* da rede. Com isso, pretende-se fornecer dados relevantes para a configuração e planejamento de redes C2 em operações militares.

A hipótese do estudo é que o *throughput* da rede diminui conforme o número de rádios configurados como nós aumenta, devido à divisão da capacidade de transmissão entre os dispositivos conectados.

1.3 Estrutura do Artigo

Na seção 1, é apresentada a introdução ao trabalho. A seção 2 detalha os métodos empregados e os cenários de teste utilizados para a coleta de dados. Na seção 3, são apresentados e discutidos os resultados obtidos nos diferentes cenários de rede. A seção 4 destaca as conclusões e explora as implicações dos resultados para redes de Comando e Controle (C2). Por fim, a seção 5 apresenta as referências consultadas ao longo do estudo.

2. METODOLOGIA

Esta seção descreve a metodologia empregada para avaliar o *throughput* do rádio Harris RF-7800M-MP operando no modo ANW2C. A metodologia é organizada em três partes: características do equipamento, com destaque às especificações técnicas relevantes para o estudo; descrição do modo de operação ANW2C, com foco nas funcionalidades que impactam o desempenho das redes; e os cenários

de teste configurados para medir o *throughput* em diferentes condições.

2.1 Características e Especificações Técnicas do Rádio Harris RF-7800M-MP

O rádio Harris RF-7800M-MP é um transceptor tático multibanda da família Falcon III. O equipamento é capaz de operar na faixa de 30 MHz a 1999,995 MHz, com modos banda larga e estreita. Ele suporta diversas formas de onda, incluindo ANW2C, AM, FM, QUICKLOOK, HAVEQUICK e TALON (HARRIS CORPORATION, 2019). Além disso, possui uma potência de transmissão máxima de 20W, GPS integrado e criptografia AES (HARRIS CORPORATION, 2019). Por sua robustez e capacidade de adaptação a diferentes cenários, o rádio apresenta características adequadas ao emprego nos mais variados ambientes operacionais.

No modo ANW2, o rádio oferece três configurações de potência para transmissão: HIGH, com 5 watts; MEDIUM, com 2 watts; e LOW, com 0,5 watts (HARRIS CORPORATION, 2014).

2.1.1 Descrição do Modo de Operação ANW2C

O modo ANW2C permite que o rádio Harris RF-7800M-MP funcione em uma rede *ad hoc* de alta velocidade, com comunicação simultânea de voz e dados. Esse modo possibilita a formação de uma rede com até 30 nós, onde cada rádio atua como um nó repetidor. Isso incrementa a robustez da rede, pois permite a continuidade das comunicações mesmo quando um ou mais elementos perdem a conectividade. No modo ANW2C a taxa de *throughput* pode alcançar até 10 Mbps em um canal de 5 MHz e até 2 Mbps em um canal de 1,2 MHz, valores que servem como referência para avaliar o desempenho da rede em condições ideais e operacionais (HARRIS CORPORATION, 2014).

2.2 Ferramenta de Medição de *Throughput*: iPerf3

Para a medição do *throughput* da rede em cada cenário de teste, utilizou-se o iPerf3, por ser amplamente empregado para realizar avaliações de desempenho de redes. O *software* é uma reimplementação em código aberto, do Iperf, inicialmente desenvolvido no *National Center for Supercomputing Applications* (NCSA). O iPerf3 permite a geração e medição de tráfego TCP e UDP, fornecendo métricas detalhadas sobre a capacidade de transferência de

dados na rede (ESNET, 2024).

O iPerf3 foi configurado para criar tráfego de dados entre os rádios Harris RF-7800M-MP, simulando as condições de operação esperadas. Segundo Mota Filho (2013), o iPerf é ideal para esses testes, pois permite simular altos volumes de tráfego para avaliar a capacidade máxima de um meio de transmissão. Essa configuração exigiu uma máquina cliente e uma máquina servidor, conectadas aos rádios, garantindo a precisão e a confiabilidade dos dados obtidos.

2.3 Definição dos Cenários de Teste

Os cenários de teste foram projetados para avaliar o impacto do aumento de rádios Harris RF-7800M-MP configurados como nós da rede sobre o *throughput*. O cenário inicial foi definido com 2 rádios, estabelecendo uma referência para o *throughput* da rede em uma configuração mínima. A partir desse ponto, o número de rádios é progressivamente aumentado em cada cenário subsequente, buscando observar como a densidade crescente de nós afeta o desempenho da rede.

No segundo cenário, 4 rádios são configurados, oferecendo uma primeira análise do impacto da duplicação do número de nós na capacidade de transmissão. Esse processo é repetido no terceiro e quarto cenários, com 8 e 20 rádios, respectivamente. Finalmente, o quinto cenário utiliza 30 rádios, atingindo o limite máximo especificado pelo manual do equipamento, o que possibilita avaliar o desempenho da rede em sua configuração máxima.

Essa abordagem gradual busca facilitar a identificação de padrões na redução de *throughput* à medida que o número de rádios aumenta.

2.4 Variáveis Controladas e Condições de Teste

Para garantir consistência e confiabilidade nos resultados, foram definidos parâmetros específicos de frequência, largura de banda, potência de transmissão e distância, considerando as características do Harris RF-7800M-MP e as regulamentações militares.

A frequência de operação foi fixada em 1430 MHz, próximo ao centro da faixa de operação do equipamento e em conformidade com as regulamentações da ANATEL para uso militar, conforme a Resolução nº 244, de 08 de dezembro de 2000 (BRASIL, 2000). Em todos os cenários, utilizou-se uma largura de banda de 5 MHz, visando atingir o *throughput* teórico máximo de 10 Mbps

(HARRIS CORPORATION, 2014).

A distância entre os rádios foi mantida em 50 metros, garantindo visada direta e ausência de obstáculos. A potência de transmissão foi ajustada para MEDIUM (2 watts), um nível intermediário para o modo ANW2C (HARRIS CORPORATION, 2014).

Devido à quantidade limitada de rádios disponíveis para os testes, em cada cenário foram empregados dois rádios configurados via software *Communications Planning Application* (CPA) para simular redes com 2, 4, 8, 20 e 30 nós. Essa abordagem permitiu uma análise prática do *throughput* mesmo com a utilização de apenas dois dispositivos físicos. Utilizou-se o *Hack RF One*, um *Software Defined Radio* (SDR), configurado como analisador de espectro, a fim de verificar a ausência de emissores externos na faixa de frequência, buscando mitigar interferências externas durante os testes.

Essas condições controladas garantem que os resultados reflitam o desempenho real da rede ANW2C nas configurações simuladas.

2.5 Procedimentos para Coleta de Dados e Análise Estatística

A coleta de dados foi realizada utilizando o *software* iPerf3, configurado para medir o *throughput* no protocolo TCP em cada cenário de teste, por um período de execução de 120 segundos para cada medição. Em cada cenário, os rádios Harris RF-7800M-MP foram configurados via CPA para simular a quantidade total de nós na rede (2, 4, 8, 20 e 30 nós), conforme os cenários estabelecidos.

Os resultados foram salvos no formato JSON, possibilitando um registro detalhado de cada teste. Em seguida, um *script* em Python foi utilizado para processar os dados e gerar gráficos, facilitando a análise visual do desempenho de *throughput* nas redes.

A análise estatística comparativa entre os cenários buscou identificar o impacto do aumento do número de nós sobre o *throughput*, fornecendo subsídios importantes para o planejamento de redes táticas de Comando e Controle (C2).

3. RESULTADOS E DISCUSSÃO

Nesta seção, são apresentados e analisados os resultados obtidos para o *throughput* da rede em cada cenário de teste, variando o número de rádios configurados como nós da rede. O objetivo foi observar a relação entre o aumento do número de nós e a variação da capacidade de transmissão média da

rede.

3.1 Resultados de *Throughput* por Cenário

Os testes de *throughput* foram realizados em cinco cenários, variando de 2 a 30 rádios configurados como nós da rede. Abaixo, são detalhados os resultados para cada cenário, incluindo as taxas médias de transferência e a quantidade total de dados transmitidos.

3.1.1 Cenário 1 (2 rádios):

No Cenário 1, com 2 rádios, o *throughput* médio foi de 3,25 Mbps, totalizando 46,9 MBytes transferidos ao longo dos 120 segundos de teste. Este valor representa a configuração mínima de nós e também o maior *throughput* observado entre todos os cenários testados (ver Figuras 1 e 2).

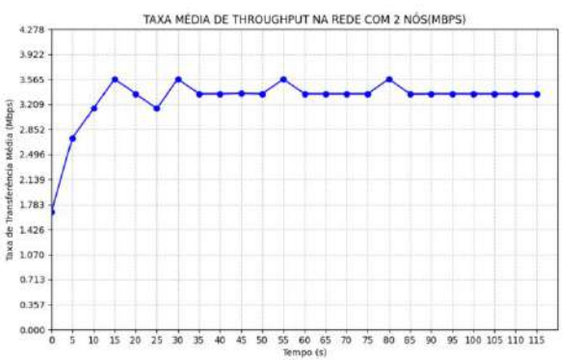


FIGURA 1 – Taxa média de *throughput* na rede com 2 nós
Fonte: Os autores

```
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-121.11 sec  46.9 MBytes  3.25 Mbits/sec
```

FIGURA 2 - Quantidade de dados transferidos e taxa de transferência em Mbps
Fonte: Os autores

3.1.2 Cenário 2 (4 rádios):

No Cenário 2, com 4 rádios, o *throughput* médio foi reduzido para 1,48 Mbps, com um total de 21,2 MBytes transferidos. Esse valor indica um impacto inicial do aumento de nós na capacidade de transmissão, representando menos da metade do *throughput* registrado no cenário 1 (ver Figuras 3 e 4).

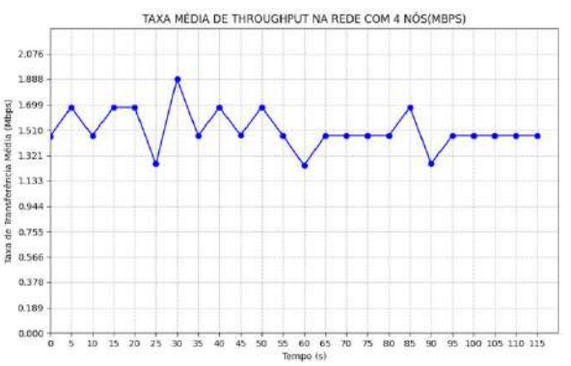


FIGURA 3 – Taxa média de *throughput* na rede com 4 nós
Fonte: Os autores

```
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-120.34 sec  21.2 MBytes  1.48 Mbits/sec
```

FIGURA 4 - Quantidade de dados transferidos e taxa de transferência em Mbps
Fonte: Os autores

3.1.3 Cenário 3 (8 rádios):

No Cenário 3, com 8 rádios, o *throughput* médio foi de 555 Kbps, com um total de 8,0 MBytes transferidos. Esse resultado continua a tendência de queda na medida em que o número de

rádios na rede aumenta (ver Figuras 5 e 6).

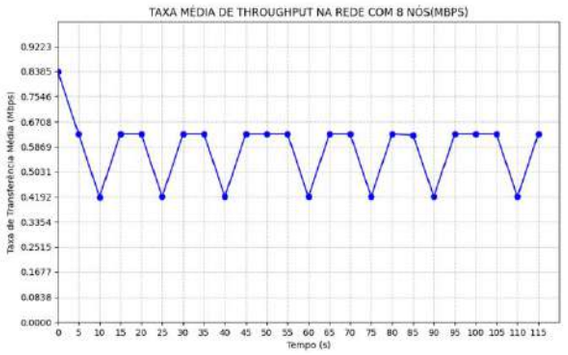


FIGURA 5 - Taxa média de *throughput* na rede com 8 nós
Fonte: Autores.

```
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-121.01 sec  8.00 MBytes   555 Kbits/sec
```

FIGURA 6 - Quantidade de dados transferidos e taxa de transferência em Mbps
Fonte: Autores.

3.1.4 Cenário 4 (20 rádios nós):

No Cenário 4, com 20 rádios, o *throughput* foi reduzido para 214 Kbps, com um total de 3,12 MBytes transferidos, indicando uma queda substancial na capacidade de transmissão à medida que a densidade de nós aumenta (ver Figuras 7 e 8).

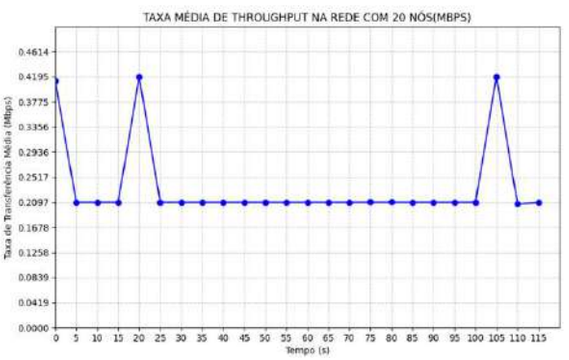


FIGURA 7 - Taxa média de *throughput* na rede com 20 nós
Fonte: Os autores

```
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-122.34 sec  3.12 MBytes   214 Kbits/sec
```

FIGURA 8 - Quantidade de dados transferidos e taxa de transferência em Mbps
Fonte: Os autores

3.1.5 Cenário 5 (30 rádios nós):

No cenário final, com o máximo de 30 rádios configurados como nós, o *throughput* médio foi de 118 Kbps e um total de 1,75 MBytes transferidos. Esse foi o menor valor registrado, refletindo a maior divisão da capacidade de transmissão entre os nós da rede e, também, a maior instabilidade na taxa de transferência observada durante o período de teste (ver Figuras 9 e 10).

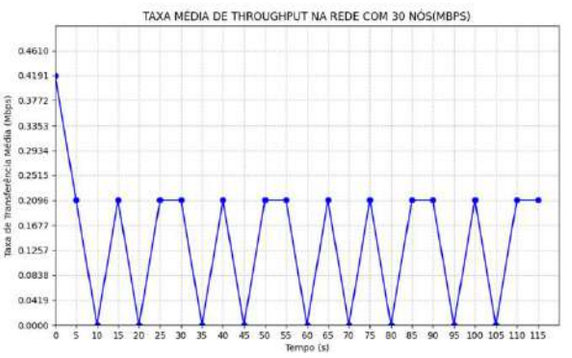


FIGURA 9 - Taxa média de *throughput* na rede com 30 nós
Fonte: Autores.

```
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-123.98 sec  1.75 MBytes   118 Kbits/sec
```

FIGURA 10 - Quantidade de dados transferidos e taxa de transferência em Mbps
Fonte: Autores.

3.1.6 Resultados preliminares

A análise dos dados confirma uma tendência de redução de *throughput* à medida que o número de rádios na rede aumenta, estabelecendo uma relação inversamente proporcional entre a

densidade de nós e a taxa de transferência obtida. Essa queda de desempenho ressalta a necessidade de um planejamento criterioso ao configurar redes de Comando e Controle (C2) em operações militares, onde um alto número de rádios pode comprometer a eficiência da rede. Esses dados fornecem uma base para otimizar a configuração de redes ad hoc, de modo a equilibrar a necessidade de conectividade com o desempenho desejado.

3.2 Análise Comparativa entre os Cenários

A comparação dos cenários testados evidencia uma queda expressiva no *throughput* à medida que o número de nós na rede aumenta. Com dois rádios, o *throughput* médio registrado foi de **3,25 Mbps**, e, ao duplicar o número para quatro rádios, esse valor caiu para **1,48 Mbps**. Essa tendência de redução progressiva se manteve nos cenários seguintes: com oito rádios, o *throughput* foi de **555 Kbps**; com vinte, **214 Kbps**; e no cenário com trinta rádios, o menor valor foi observado, com apenas **118 Kbps**. Esses resultados sugerem que o *throughput* decresce de forma não linear, embora a queda seja superior e próximo de 50% todas as vezes em que o número de nós foi duplicado (ver Figura 11).

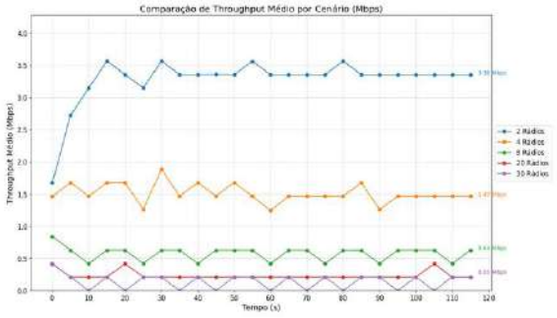


FIGURA 11 – Comparação de *throughput* por cenário
Fonte: Autores.

Esse padrão de degradação destaca a necessidade de ajuste na quantidade de rádios para manter um desempenho aceitável em redes de maior densidade.

3.3 Discussão dos Fatores de Impacto no *Throughput*

Os resultados indicam que o *throughput* é diretamente afetado pelo aumento no número de rádios, com uma redução significativa na capacidade de transmissão conforme mais nós são adicionados. Em redes *ad hoc* como as configuradas no modo ANW2C, a largura de banda disponível é compartilhada entre os nós, e o aumento de tráfego de retransmissão reduz a eficiência da transmissão.

3.3.1 Efeito do Número de Rádios no *Throughput*

A análise dos cenários confirma que o aumento no número de rádios impacta negativamente o *throughput* médio da rede. Nos cenários de teste, o *throughput* foi reduzido de 3,25 Mbps com dois rádios para apenas 118 Kbps com trinta rádios, refletindo a limitação da largura de banda compartilhada e o aumento da carga de retransmissão em redes *ad hoc*. Esse comportamento destaca a importância de balancear a quantidade de rádios com a necessidade de *throughput* necessário na rede.

3.3.2 Interferências e Condições Ambientais

Embora os testes tenham sido precedidos pela verificação da ausência de emissores externos na faixa de frequência utilizada, a possibilidade de interferências não pode ser descartada. Não foi utilizada uma câmara anecoica, portanto, não houve isolamento de fontes externas de ruído e nem de reflexões do sinal. O impacto residual de fatores externos, caso presente, pode ter contribuído para pequenas variações nos resultados obtidos. Entretanto, considerou-se que o ambiente de teste foi favorável e semelhante ao emprego do equipamento em situações reais. A garantia de uma faixa livre de interferências reforça a confiabilidade dos dados, mas o impacto de condições ambientais imprevistas ainda deve ser considerado em testes futuros.

3.4 Limitações do Estudo

Este estudo enfrentou algumas limitações, sendo a principal a quantidade reduzida de rádios disponíveis, o que exigiu a simulação de nós adicionais por meio do *software* CPA. Embora essa abordagem tenha permitido uma análise viável, o uso de apenas dois rádios para representar redes de até 30 nós pode introduzir variações na representação do desempenho real da rede. Além disso, as medições de *throughput* foram limitadas ao protocolo TCP e a um tempo de execução fixo de 120 segundos, o que pode não capturar completamente as variações de desempenho em diferentes condições de carga de tráfego.

Essas limitações indicam que, para uma análise mais completa, estudos futuros poderiam incluir uma maior quantidade de rádios físicos, além de testes com diferentes protocolos e tempos de execução variáveis. Tais ajustes contribuiriam para validar os resultados e ampliar a compreensão sobre o comportamento de *throughput*

nas redes estabelecidas por meio do rádio Harris RF-7800M-MP no modo ANW2C.

4. CONCLUSÕES

Este estudo investigou o impacto do número de rádios Harris RF-7800M-MP, operando no modo ANW2C, sobre a capacidade de transmissão da rede. Os resultados revelaram uma relação inversamente proporcional entre o número de nós e o *throughput da rede*, evidenciada pelas quedas significativas nas taxas de transmissão conforme a densidade da rede aumentava. Esses dados fornecem uma base valiosa para o planejamento e a otimização de redes no modo ANW2C.

4.1 Revisão dos Objetivos e Hipótese

O objetivo principal deste estudo foi avaliar o efeito do aumento no número de rádios Harris RF-7800M-MP sobre o *throughput* da rede, operando no modo ANW2C. A hipótese de que o *throughput* diminuiria conforme a densidade de rádios na rede aumentasse foi confirmada, com uma queda substancial na capacidade de transmissão observada em cada cenário testado. Esses achados validam a hipótese e destacam a necessidade planejamento para maximizar a eficiência das redes de C2 em campo.

4.2 Conclusões Principais

Os testes realizados indicaram que, para cada duplicação de rádios na rede, o *throughput* apresentou uma queda expressiva, evidenciando a limitação da largura de banda compartilhada e o aumento da carga de retransmissão inerentes às redes *ad hoc*. Utilizando-se dois rádios, o *throughput* médio foi de **3,25 Mbps**, e, no cenário com trinta rádios, foi reduzido para **118 Kbps**. Esse padrão de redução confirma que a densidade elevada de nós compromete o desempenho da rede, o que reforça a importância de um planejamento adequado para balancear o número de rádios com as necessidades de taxa de transmissão.

4.3 Sugestões Para Trabalhos Futuros

Para aprofundar o conhecimento sobre o comportamento do *throughput* em redes *ad hoc* militares, recomenda-se:

- **Variedade de Protocolos**: Ampliar os testes para incluir diferentes protocolos, como UDP, para avaliar as variações de *throughput* e latência em condições distintas de tráfego

- **Utilizar Outras Frequências na Faixa de Operação do Rádio:** Conduzir testes em diferentes frequências dentro da faixa operacional do rádio, para verificar se a diminuição do *throughput* apresenta variações em outras faixas.
- **Aumento da Quantidade de Rádios Físicos**: Realizar testes com um maior número de rádios físicos para validar os resultados obtidos com simulação, o que possibilitará uma representação ainda mais precisa do desempenho da rede.

Essas sugestões buscam auxiliar os futuros trabalhos a otimizar redes de C2 e aumentar a resiliência e eficiência das comunicações em operações militares.

IMPACT OF NODE DENSITY ON THE THROUGHPUT OF THE HARRIS RF-7800M-MP RADIO IN ANW2C MODE

Abstract: This study analyzes the throughput of the Harris RF-7800M-MP radio operating in ANW2C mode, evaluating the impact of increasing the number of radio nodes on network transmission capacity. Tests were conducted across five scenarios with varying numbers of radios, ranging from 2 to 30 nodes, configured with an intermediate transmission power of 2 watts, at a distance of 50 meters and in direct line of sight. The frequency of 1430 MHz and a bandwidth of 5 MHz were used, complying with military usage regulations, aiming to reach the theoretical maximum throughput of 10 Mbps under ideal conditions. Data collection was performed using iPerf3 software, with practical throughput analysis through simulations that considered the physical limitations of the devices. The results indicated a progressive decrease in throughput as the number of radios in the network increased, highlighting the need for proper planning in configuring Command and Control (C2) networks in military operations.

Index Terms: Throughput. Harris RF-7800M-MP radio. ANW2C mode. Ad hoc networks. Tactical communications.

REFERÊNCIAS

ANATEL, Agência Nacional de Telecomunicações. **Mapeamento de Resoluções Vigentes e Revogadas da ANATEL.** Disponível em: <https://sistemas.anatel.gov.br/anexar-api/publico/anexos/download/48d1d2bbb8964944745e282888e905b2>. Acesso em: 22 outubro 2024.

BBC. **Guerra eletrônica: o temido e sombrio papel da guerra eletrônica no conflito da** Ucrânia, 28 fevereiro 2022. Disponível em: <https://www.bbc.com/portuguese/internacional-60551648>. Acesso em: 31 outubro 2024.

BRASIL, Agência Nacional de Telecomunicações. **Resolução nº 244, de 8 de dezembro de 2000 (distribuição radiofrequências para fins militares)**. Brasília, DF.

DUPUY, R. **Network performance measurement with iPerf3**. New York: O'Reilly Media, 2017.

HARRIS CORPORATION. **RF-7800M-MP multiband networking manpack radio datasheet.** Melbourne. 2019. Disponível em: <https://www.l3harris.com/sites/default/files/2021-01/cs-tcom-falcon-iii-rf-7800m-mp-multiband-networking-manpack-radio-datasheet.pdf>. Acesso em: 30 outubro 2024.

HARRIS CORPORATION. **RF Communication Division. Falcon III RF-7800M-MP multiband networking manpack radio – Operation Manual**. Rochester, NY. 2014.

MOTA FILHO, João Eriberto. **Análise de tráfego em redes TCP/IP: utilize tcpdump na análise de tráfegos em qualquer sistema operacional**. São Paulo, SP. Novatec Editora, 2013.

MICROSOFT. **The Cyber and Influence Operations of the War in Ukraine's Digital Battlefield, 2022.** Disponível em: <https://www.microsoft.com/pt-br/security/security-insider/intelligence-reports/the-cyber-and-influence-operations-of-the-war-in-ukraines-digital-battlefield/>. Acesso em: 31 outubro 2024.

ARMY, United States. **Russian Cyber Operations in the Invasion of Ukraine. Cyber Defense Review, 2022.** Disponível em: <https://cyberdefensereview.army.mil/Portals/6/Documents/2022_fall/02_Lin.pdf?ver=YqkqyveSz8G2nNU0_sxVqQ%3D%3D>. Acesso em: 31 outubro 2024.

APÊNDICE A – *SCRIPT* EM PYTHON PARA GERAÇÃO DE GRÁFICOS DE *THROUGHPUT*

Este apêndice apresenta o script em Python utilizado para transformar os resultados do IPerf3, armazenados no formato resultados.json, em gráficos que representam a taxa média de transferência a cada 5 segundos. O objetivo foi calcular a média do *throughput* ao longo dos intervalos, exibindo os valores em Mbps para facilitar a interpretação dos dados.

Script em Python para Geração de Gráficos de *Throughput*:

```
import json
import matplotlib.pyplot as plt
import numpy as np

# Carregar os dados do arquivo JSON
with open('resultados.json', 'r') as file:
    data = json.load(file)

# Definir a duração do intervalo em segundos e listas para armazenar as médias
interval_duration = 5
timestamps = []
transfer_rates_mbps = []

# Coletar as taxas de transferência em Mbps para cada segundo
rates_per_second = [interval['sum']['bits_per_second'] / 1_000_000 for interval in data['intervals']]

# Calcular a média de throughput a cada 5 segundos
for i in range(0, len(rates_per_second), interval_duration):
    avg_rate = np.mean(rates_per_second[i:i + interval_duration])
    timestamps.append(i)
    transfer_rates_mbps.append(avg_rate)
```

```
        # Criar o gráfico com melhorias para visualização
        plt.figure(figsize=(10, 6))
        plt.plot(timestamps, transfer_rates_mbps, marker='o', linestyle='-', color='b')

        # Melhorias para facilitar a interpretação do gráfico
        plt.title('Taxa Média de Transferência da Rede a Cada 5 Segundos (Mbps)')
        plt.xlabel('Tempo (s)')
        plt.ylabel('Taxa de Transferência Média (Mbps)')
        plt.grid(True, linestyle='--', alpha=0.7)
        plt.xlim(0, max(timestamps) + 5)
        plt.ylim(0, max(transfer_rates_mbps) * 1.2)
        plt.xticks(range(0, max(timestamps) + 5, 5))
        plt.yticks(np.arange(0, max(transfer_rates_mbps) * 1.2,
max(transfer_rates_mbps) / 10))

        # Exibir o gráfico
        plt.show()
```

Explicação do Script:

Carregamento e Processamento dos Dados: Os dados de *throughput* são carregados do arquivo JSON gerado pelo IPerf3. A taxa de transferência é convertida de bits por segundo para Mbps.

Cálculo das Médias por Intervalo: Para reduzir a oscilação dos valores de *throughput*, o script calcula a média da taxa de transferência a cada 5 segundos.

Geração do Gráfico: O gráfico exibe a taxa média de transferência ao longo do tempo, com marcações e melhorias visuais, como grelha ajustável, limites de eixo e rótulos, para uma compreensão mais clara dos resultados de *throughput* em cada cenário.

DESENVOLVIMENTO DE UMA FERRAMENTA DE CRIPTOGRAFIA DE DADOS PRODUÇÃO DE UMA FERRRAMENTA DE CRIPTOGRAFIA E DESCRIPTOGRAFIA PARA PROTEÇÃO DE DADOS ATRAVÉS DE UMA INTERFACE GRÁFICA

Cap **Flávio** Barros Correia
Cap Diego Madureira **Peixoto**
Cap Cassius Matheus Alves **Bierhals**

RESUMO

Este estudo tem por finalidade fornecer informações que possam contribuir para o desenvolvimento de uma ferramenta de criptografia e descriptografia de dados que atendam às demandas das operações militares conduzidas pelo Exército Brasileiro. A partir de uma análise sumária, da literatura existente sobre o tema, serão definidos os requisitos para o desenvolvimento de uma ferramenta que implementa algoritmos de criptografia e descriptografia em uma interface gráfica, garantindo segurança, desempenho e simplicidade para que o usuário final possa proteger suas informações das diversas ameaças cibernéticas atuais, de forma eficiente e segura.

Palavras-chave: criptografia, algoritmo, dados, segurança, exército

1 INTRODUÇÃO

A finalidade deste trabalho é apresentar como produto final uma aplicação digital que seja capaz de criptografar e descriptografar dados com uma interface gráfica intuitiva que atenda às necessidades de uma operação militar do Exército Brasileiro.

1.1 CONTEXTUALIZAÇÃO DO ESTUDO

Criptografar uma informação consiste em torná-la ininteligível para quem não deveria possuir acesso a ela. É essencial para qualquer instituição que precise manter sigilo sobre seus dados ou protegê-los de potenciais ameaças cibernéticas.

Com o avanço da tecnologia e o advento da Guerra Cibernética, torna-se fundamental a criação de medidas de proteção que garantam a segurança da informação no âmbito do Exército Brasileiro, sobretudo nas operações militares.

Os desafios de gerenciar riscos, evitar ameaças e mitigar danos estão essencialmente conectados ao estabelecimento de uma rede de comunicações segura e eficiente.

Diante desta realidade, faz-se necessário o fortalecimento da mentalidade de segurança da informação. O desenvolvimento de uma ferramenta de criptografia de dados confiável e de fácil operação é uma maneira concreta de contribuir para esta mentalidade.

1.2 JUSTIFICATIVA

O Exército Brasileiro, enquanto uma das instituições responsáveis pela defesa da soberania nacional, deve estar constantemente capacitado para garantir que seus dados permaneçam inacessíveis para usuários não autorizados.

Uma falha de segurança que prejudique o princípio da confidencialidade das informações pode colocar em circulação inapropriada desde detalhes operacionais e logísticos até dados sensíveis sobre a tropa.

Assegurar a proteção de dados é um fator determinante, tanto para a manutenção da imagem da Força, quanto para a segurança e a eficácia de uma operação militar.

1.3 DEFINIÇÃO DO PROBLEMA DE PESQUISA

A evolução dos meios tecnológicos aumenta a demanda por sistemas de segurança e exige que as ferramentas existentes de segurança da informação estejam constantemente se atualizando.

Paralelo a este fator, faz-se necessária a

adaptação desses recursos às necessidades das operações militares do Exército Brasileiro, de modo que possam ser empregados, inclusive, por indivíduos não qualificados, através de uma aplicação que indique intuitivamente as etapas de um processo de criptografia ou descriptografia de uma informação.

1.4 OBJETIVOS DA PESQUISA

Esta pesquisa busca contribuir para o desenvolvimento de uma ferramenta de criptografia que atenda às demandas de proteção de dados por parte do Exército Brasileiro contra potenciais ameaças internas e externas em operações militares.

1.5 ESTRUTURA DO CONTEÚDO ESCRITO

O artigo em sua primeira seção contextualiza a importância da criptografia no campo da proteção cibernética, abordando os princípios da segurança da informação.

A Revisão de Literatura apresenta conceitos importantes para o estudo tais como os de criptografia simétrica e assimétrica, alguns dos principais algoritmos de criptografia, - AES (Advanced Encryption Standard) e RSA (Rivest-Shamir-Adleman) - oferecendo uma análise comparativa de sua eficiência e segurança, e o conceito de *hash* Serão incluídas referências a autores conceituados sobre segurança em redes de computadores e criptografia, que exploram essas ideias.

Na seção de Métodos de Pesquisa, será apresentada a concepção geral da ferramenta a ser desenvolvida. Serão identificadas as funcionalidades essenciais que a aplicação deve possuir, as etapas do processo de criptografia e descriptografia e a criação de uma interface gráfica intuitiva. Um exemplo prático seria a inclusão de uma funcionalidade para criptografar e descriptografar arquivos como documentos PDF, diretamente pela interface. Os dados coletados para avaliação da eficácia da ferramenta serão obtidos por meio de testes da mesma por potenciais usuários.

A seção de Implementação abordará as tecnologias utilizadas, como *Python* para a programação da ferramenta e o uso de bibliotecas como *PyCryptodome* para a implementação dos algoritmos de criptografia. Já a seção sobre a Interface Gráfica explicará a criação de um design intuitivo utilizando *frameworks* como *Tkinter*.

Na parte de Testes de Segurança e Desempenho, serão detalhados os testes realizados para avaliar a robustez da ferramenta contra-ataques de força bruta e o tempo de processamento em diferentes cenários.

Por fim, a Documentação e POP (Procedimentos Operacionais Padrão) apresentarão as instruções de uso e manutenção da ferramenta, acompanhada de exemplos práticos de utilização em operações militares.

2 DESENVOLVIMENTO

2.1 REVISÃO DA LITERATURA

A criptografia é uma forma de segurança que permite a troca segura de informações em um mundo ameaçado. Para Schneier (1996, p. 21), “é a arte e a ciência de manter mensagens seguras” (tradução nossa).

O processo de criptografar uma informação consiste em torná-la inacessível para um indivíduo não autorizado. É uma prática que busca manter a confidencialidade, a autenticidade e a integridade de um dado.

A criptografia é essencial para proteger dados sensíveis que circulam em redes de comunicação, especialmente em situações de combate ou operações de inteligência. Não por acaso, como explica Tanenbaum (2011, p. 148), os militares tiveram papel importante no desenvolvimento dessa arte e definiram as bases para futuras tecnologias.

2.1.1 CRIPTOGRAFIA SIMÉTRICA

Explica Stallings (2015, p. 21), que a criptografia simétrica ou de chave privada, é uma técnica em que a mesma chave é utilizada para cifrar e decifrar dados, exigindo que ambas as partes da comunicação compartilhem essa chave de forma segura.

A utilização de uma chave criptográfica única permite a implementação deste método de segurança de maneira facilitada e é preferível para situações que priorizem a velocidade e a maior quantidade de

informação, por conta do menor consumo de recursos dos equipamentos disponíveis.

Ferguson, Schneier e Kohno concordam que (2010, p. 28) a criptografia simétrica oferece maior eficiência computacional, sendo adequada para sistemas onde há grande volume de dados a serem processados em tempo real.

FIGURA 1 - Criptografia Simétrica.

Fonte: os autores.

2.1.2 AES (*ADVANCED ENCRYPTION STANDARD*)

O algoritmo AES foi desenvolvido como um sucessor ao algoritmo DES (*Data Encryption Standard*), que se tornou vulnerável a ataques de força bruta devido ao aumento das capacidades operacionais dos equipamentos modernos.

Diante deste novo cenário, o AES foi projetado para ser rápido, seguro e eficiente, com a capacidade de operar com chaves de diferentes tamanhos, o que aumenta sua segurança contra-ataques.

Buscando transpor este obstáculo da vulnerabilidade a ataques de força bruta, o algoritmo AES foi estruturado para operar com três tamanhos de chave: 128, 192 e 256 bits, enquanto o anterior, DES, destinava 56 bits da chave para a cifração da informação.

A principal vantagem do AES é a sua robustez contra-ataques de força bruta, sendo que, com chaves de 256 bits, o número de possíveis combinações torna praticamente inviável qualquer tentativa de quebra do algoritmo com a tecnologia atual.

O algoritmo AES, desta maneira, conforme Daemen e Rijmen (2002, p. 147) permite uma grande flexibilidade no comprimento do bloco sem perder as propriedades de eficiência e alta resistência contra criptoanálise. Este equilíbrio entre segurança e desempenho, permite sua aplicação em várias plataformas e protocolos, desde dispositivos móveis até redes de alto desempenho.

TABELA 1 - Estimativas para ataques de 'força bruta' em algoritmos simétricos.

Custo	56 bits	64 bits	112 bits	128 bits
$100 K	3,5 horas	37 dias	10^13 anos	10^18 anos
$1 M	21 minutos	4 dias	10^12 anos	10^17 anos
$10 M	2 minutos	9 horas	10^11 anos	10^16 anos
$100 M	13 segundos	1 hora	10^10 anos	10^15 anos
$1 G	1 segundo	5,4 minutos	10^9 anos	10^14 anos
$10 G	0,1 segundos	32 segundos	10^8 anos	10^13 anos
$100 G	0,01 segundos	3 segundos	10^7 anos	10^12 anos
$1 T	1 milissegundo	0,3 segundos	10^6 anos	10^11 anos

Fonte: NAKAMURA, Emílio Tissato. GEUS, Paulo Lício de. *Segurança de Redes em Ambientes Corporativos*. 1ª. ed. São Paulo: Novatec Editora, 2007. Reimpro. 2012, Tabela 9.3, p. 311. Estimativas para ataques de 'força bruta' em algoritmos simétricos.

2.1.3 CRIPTOGRAFIA ASSIMÉTRICA

Stallings (2015, p. 200) afirma que a criptografia assimétrica ou de chave pública oferece uma mudança radical no processo anterior, já que, ao contrário da criptografia simétrica, não requer que as partes envolvidas compartilhem uma chave secreta.

Esse método de proteção de dados faz uso de um par de chaves nas suas operações: uma chave privada e uma chave pública. Esta pode ser compartilhada abertamente e utilizada para criptografar os dados que se deseja transmitir por um canal de comunicação seguro; aquela deve ser mantida com seu proprietário e utilizada para decifrar os dados recebidos.

"A principal vantagem de tais sistemas é que fornecer chaves públicas autênticas é geralmente mais fácil do que distribuir chaves secretas de uma forma segura, conforme exigido em sistemas de chaves simétricas" (MENEZES, VAN OORSCHOT e VANSTONE, 1996 , p. 283, tradução nossa).

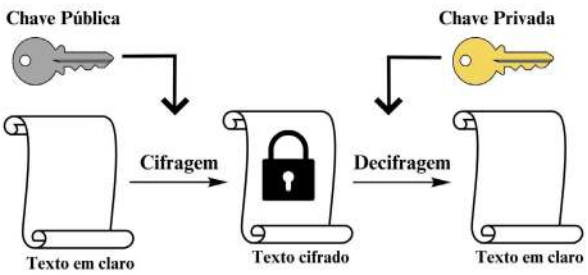
Sua escolha está relacionada às operações que não demandam grande volume de dados ou velocidade, uma vez que consome mais recursos computacionais.

Outra vantagem dessa forma de criptografia é a garantia do princípio de autenticidade da informação. Além de ser necessário o par de chaves do destinatário para que o conteúdo seja devidamente cifrado e decifrado, o par de chaves do remetente

pode ser utilizado para assinar digitalmente a mensagem com a sua chave privada. Dessa maneira, o destinatário, de posse da chave pública do remetente, terá condições de verificar se ela foi enviada por ele.

"As assinaturas digitais permitem um método de assegurar que a mensagem é autêntica para um usuário e que ela de fato se origina da pessoa que alega tê-la enviado" (PAAR e PELZL, 2010, p. 259, tradução nossa). Schneier (1996, p. 62) as compara com as assinaturas manuscritas, como prova de autenticidade.

FIGURA 2 - Criptografia assimétrica.



Fonte: os autores.

2.1.4 RSA (RIVEST-SHAMIR-ADLEMAN)

O algoritmo RSA, Rivest-Shamir-Adleman, se baseia na dificuldade de fatoração de números inteiros grandes, razão pela qual, segundo Stallings (2015, p. 207), desde o seu desenvolvimento segue como a técnica de uso geral mais aceita e implementada para a encriptação de chave pública.

O processo criptográfico do algoritmo se inicia com a seleção de dois números primos grandes, com centenas de dígitos. O produto da multiplicação entre esses dois números gera um valor que será usado nas operações matemáticas seguintes para criar o par de chaves, pública e privada, garantindo a segurança e a integridade da comunicação.

Pela própria natureza matemática do problema, o tempo exponencial para resolvê-lo torna a operação em questão impraticável, mesmo para os computadores mais avançados tecnologicamente.

"Fazendo com que cada um dos fatores tenha 100 dígitos, a multiplicação pode ser feita em uma fração de segundo, mas a fatoração exigiria bilhões de anos, usando o melhor algoritmo conhecido" (HELLMAN, 1978, p. 45, tradução nossa).

Em concordância com Katz e Lindell (2007, p. 231), que relacionam a criptografia moderna a problemas matemáticos, o RSA exemplifica a eficácia da teoria dos números aplicada ao contexto de segurança da informação.

"Ainda que os algoritmos de fatoração estejam constantemente se desenvolvendo, a situação atual ainda está longe de representar uma ameaça para a segurança do RSA, quando ela é usada adequadamente" (BONEH, 1999, p. 204, tradução nossa).

TABELA 2 - Fatoração de chaves do algoritmo assimétrico.

Nº bits	MIPS/Anos necessários	Tempo p/ Pentuim II – 300 MHz
512	< 200	8 meses
728	100.000	300 anos
1024	3 x 107	105 anos
1280	3 x 109	107 anos
1536	2 x 1011	108 anos
2048	4 x 1014	1,3 x 1012 anos

Fonte: NAKAMURA, Emílio Tissato. GEUS, Paulo Lício de. *Segurança de Redes em Ambientes Corporativos*. 1ª. ed. São Paulo: Novatec Editora, 2007. Reimpr. 2012, Tabela 9.4, p. 311. Fatoração de chaves do algoritmo assimétrico.

2.1.5 HASHING

A técnica de *Hashing,* ou geração de *hash*, consiste em transformar, com processos matemáticos, dados de tamanho variável em uma saída de tamanho fixo, a qual se dá o nome de *hash.* Segundo Rivest (1992, p. 5), as funções *hash* (ou *digest*) são utilizadas para criar "impressões digitais" de dados, permitindo que grandes quantidades de informação sejam resumidas em um pequeno valor fixo.

O *hash* gerado é composto de uma sequência de caracteres única, resultado de uma operação unilateral. Isso significa que sua reversão é altamente improvável, uma vez que deveriam ser testadas todas as combinações possíveis para obter a entrada original.

Pelo mesmo motivo de que a quantidade de combinações possíveis para gerar um *hash* dificulta sua reversão, também torna bastante improvável que duas entradas diferentes gerem a mesma saída, ou seja, uma colisão. Apesar de ser possível, os algoritmos modernos são projetados para serem

resistentes a essa remota possibilidade, como por exemplo o algoritmo SHA-256.

"Um hash é um exemplo do que é chamado de função unidirecional, uma função fácil de calcular, mas difícil de inverter, para que a mensagem original não possa ser recuperada" (DIFFIE e LANDAU, 2007, p. 253, tradução nossa).

Essa técnica garante ainda que com a menor alteração nos dados, o *hash* seja alterado completamente. Essa é mais uma maneira de verificar a integridade da informação.

TABELA 3 - O espaço das chaves e o tempo de processamento necessário.

Combinações permitidas	7 bBytes	7 bBytes	8 bBytes	8 bBytes
Letras minúsculas (26)	8 x 10^9	2,2 horas	2,1 x 10^11	2,4 dias
Minúsculas e dígitos (36)	7,8 x 10^10	22 horas	2,8 x 10^12	33 dias
Alfanuméricos (62)	3,5 x 10^12	41 dias	2,2 x 10^14	6,9 anos
Caracteres imprimíveis (95)	7 x 10^13	2,2 anos	6,6 x 10^15	210 anos
Caracteres ASCII (128)	5,6 x 10^14	18 anos	7,2 x 10^16	2300 anos
Caracteres ASCII de 8 bits (256)	7,2 x 10^16	2300 anos	1,8 x 10^19	580000 anos

Fonte: NAKAMURA, Emílio Tissato. GEUS, Paulo Lício de. *Segurança de Redes em Ambientes Corporativos*. 1ª. ed. São Paulo: Novatec Editora, 2007. Reimpr. 2012, Tabela 9.2, p. 310. Fatoração de chaves do algoritmo assimétrico.

2.1.6 PROTEÇÃO DAS COMUNICAÇÕES MILITARES

O desafio da implementação de um sistema de criptografia adequado também é preocupação da Força Terrestre. É um requisito básico para que as operações militares ocorram sem o risco de comprometimento.

A importância da proteção cibernética se dá desde os escalões mais altos, com, por exemplo, a definição de uma Doutrina Militar de Defesa Cibernética (MD31-M-07, 2023), até os níveis mais elementares.

Conforme a Diretriz Estratégica Organizadora do Sistema de Comando e Controle do Exército (EB10-D-01.013, 2021), "a criptografia deve ser empregada de forma extensiva para garantir a segurança da informação e a proteção dos dados críticos em redes de comando e controle" (p. 22).

A segurança cibernética também é abordada no Manual de Guerra Cibernética (EB70-MC-10.232, 2017), que destaca a necessidade de uma infraestrutura cibernética resiliente capaz de suportar ataques e manter a continuidade das operações de comando e controle. O uso do algoritmo AES no Sistema de Comando e Controle da Força Terrestre e em outros sistemas de comunicação demonstra a adaptação do Exército Brasileiro às melhores práticas globais de segurança da informação.

O crescimento das ameaças cibernéticas e dos ataques direcionados a infraestruturas críticas incentiva as Forças Armadas a adotarem uma abordagem proativa no que tange à proteção cibernética.

2.2 MÉTODOS DE PESQUISA

2.2.1 ABORDAGEM

A metodologia seguiu uma abordagem empírica e exploratória, visando implementar soluções robustas de criptografia de dados que garantem a confidencialidade, integridade e autenticidade das informações em cenários críticos. A pesquisa combinou uma revisão bibliográfica com desenvolvimento prático, permitindo identificar e aplicar melhores práticas em segurança cibernética.

2.2.2 DESENVOLVIMENTO DA FERRAMENTA

Através da aplicação *Visual Studio Code*, que permite a edição de códigos de programação, foi desenvolvido em linguagem *Python* um executável que permita a criptografia ou descriptografia baseada em uma combinação dos dois algoritmos referenciados.

O algoritmo AES-256 é utilizado para garantir a confidencialidade e a integridade dos dados transmitidos, enquanto o algoritmo RSA-4096 é empregado no gerenciamento das chaves simétricas geradas. Esta conjunção proporciona o equilíbrio ideal entre segurança e eficiência para a criação de um método robusto de segurança de dados sensíveis.

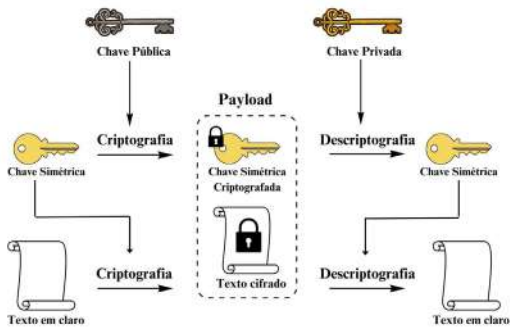
Além dos algoritmos principais, a pesquisa também investigou soluções

complementares, como derivação de chaves seguras e assinaturas digitais. Essas técnicas adicionaram camadas extras de proteção e garantiram a autenticidade das informações, evitando modificações maliciosas durante a transmissão.

O desenvolvimento da solução seguiu um processo gradual, com ajustes realizados conforme necessário ao longo da implementação. Essa abordagem possibilitou uma integração eficiente entre teoria e prática, assegurando que os algoritmos selecionados fossem adequados e atendessem aos requisitos do estudo. A criptografia simétrica (AES-256) foi utilizada para lidar com grandes volumes de dados, enquanto a criptografia assimétrica (RSA-4096) garantiu a proteção das chaves simétricas.

Por fim, a inclusão de assinaturas digitais assegurou a integridade e autenticidade das informações trocadas, resultando em uma solução equilibrada entre segurança e eficiência. A metodologia aplicada garantiu que a solução atendesse às necessidades de segurança em ambientes críticos, como centros de controle e infraestruturas sensíveis.

FIGURA 3 - Criptografia híbrida.



Fonte: os autores.

2.3 APRESENTAÇÃO E ANÁLISE DE DADOS

2.3.1 IMPORTAÇÃO DAS BIBLIOTECAS

A primeira etapa no desenvolvimento do *script* é a importação de bibliotecas necessárias para garantir que todas as funcionalidades da ferramenta de criptografia estejam disponíveis. Cada biblioteca desempenha um papel essencial para o funcionamento adequado da ferramenta, conforme a Tabela 1.

TABELA 4 - Bibliotecas

BIBLIOTECA	FINALIDADE
Tkinter	Criar uma interface gráfica que facilita a interação com o usuário, através de elementos como janelas, botões e caixas de diálogo
PyCryptodome	Fornecer os algoritmos de criptografia e *hash* utilizados
Base64	Converter dados binários (como o arquivo criptografado) para um formato de texto legível
OS	Permitir a manipulação de arquivos e caminhos de arquivos
Datetime	Registrar a data e a hora em que as operações são realizadas, para fins de auditoria e rastreamento

Fonte: os autores

2.3.1 FUNÇÕES

As funções são os elementos que conduzem a operação do *script*. A exposição procurou seguir uma sequência lógica que acompanhe o funcionamento do programa. Conforme a próxima função é acionada, o trabalho fornece sua explicação respectiva.

O código completo e as instruções de uso da aplicação estão disponíveis no Apêndice A deste estudo.

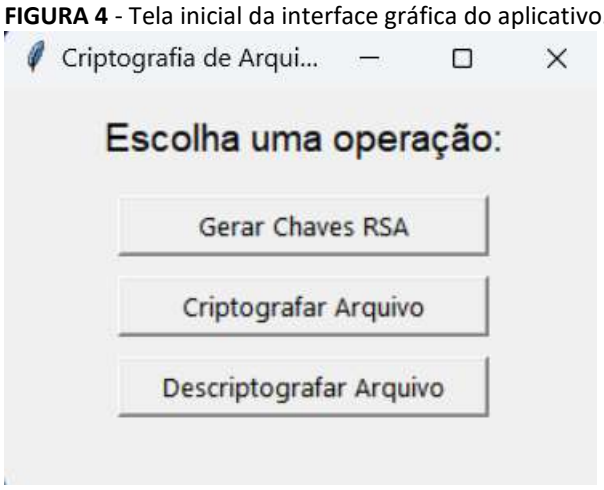
2.3.1.1 INÍCIO DO SCRIPT E CRIAÇÃO DA INTERFACE GRÁFICA

O programa deve ser executado diretamente pelo usuário. Caso não haja erros na execução, a interface gráfica criará uma janela para interação com o usuário.

As opções são apresentadas de forma simples e intuitiva para fácil entendimento do usuário. Cada um dos botões é responsável por

acionar uma função específica: gerar chaves RSA, criptografar e descriptografar arquivos.

FIGURA 4 - Tela inicial da interface gráfica do aplicativo.



Fonte: os autores.

2.3.1.2 GERAR CHAVES RSA

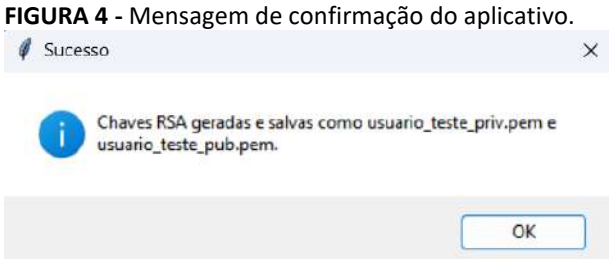
A função do primeiro botão é a geração de um par de chaves utilizando o algoritmo RSA, de criptografia assimétrica.

O programa solicitará um nome a ser usado para salvar os arquivos que contém a chave privada e a chave pública. A chave privada, por sua vez, deverá ser protegida por meio de uma senha também fornecida e confirmada pelo usuário.

Ambas as chaves são geradas por meio do algoritmo RSA com 4096 bits de comprimento. A chave privada será protegida pelo algoritmo AES com 128 bits, fornecendo mais uma camada de segurança.

Ao final da execução, o programa exibe uma mensagem de confirmação do usuário e o par de chaves é salvo no mesmo diretório do *script*.

FIGURA 4 - Mensagem de confirmação do aplicativo.



Fonte: os autores.

2.3.1.3 CRIPTOGRAFAR ARQUIVO

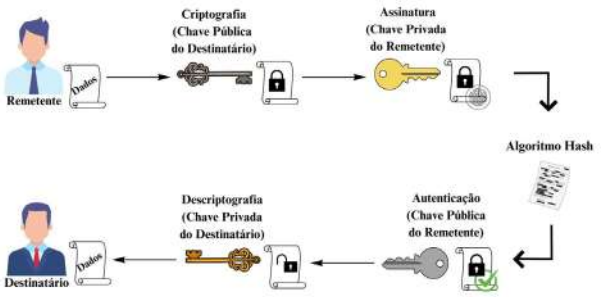
O segundo botão ativa a função para encriptar o arquivo a ser selecionado pelo usuário. Para esta operação é necessário que as chaves sejam geradas na etapa anterior.

O programa, com o algoritmo AES-256, gera uma nova chave simétrica, que é usada para cifrar o arquivo selecionado. Foi inserido como recurso adicional o modo GCM (*Galois/Counter Mode*), que cria uma espécie de *tag* de autenticação que detecta qualquer modificação no arquivo após a criptografia. Se for detectada alguma alteração, a etapa da descriptografia não poderá ser realizada corretamente.

Conforme o funcionamento da criptografia híbrida, a chave pública do destinatário é utilizada para cifrar a segunda chave simétrica, que foi criada nessa mesma etapa, enquanto a chave privada do remetente funciona como assinatura digital, para certificar que o arquivo foi enviado pelo usuário correto.

O arquivo final criptografado é composto pelos seguintes elementos: o próprio conteúdo do arquivo (cifrado com a chave AES-256), a chave AES-256 (cifrada pela chave pública do destinatário), a *tag* de autenticação (gerada pelo modo de operação GCM) e a assinatura digital. O produto é salvo no mesmo diretório com a extensão '.enc' e o programa exibe ao usuário uma mensagem de confirmação.

FIGURA 5 - Processo de criptografia assimétrica com assinatura digital e autenticação com as chaves pública e privada.



Fonte: os autores.

2.3.1.4 DESCRIPTOGRAFAR ARQUIVO

A terceira e última alternativa que a aplicação disponibiliza opera a decifração de um arquivo previamente criptografado. Semelhante à etapa anterior, é necessário importar a chave privada do destinatário e a

chave pública do remetente junto com o arquivo a ser decifrado.

A ferramenta, de posse da chave privada do destinatário, descriptografa o conteúdo do arquivo. Durante esse processo, a *tag* de autenticação é verificada: se houver qualquer alteração no arquivo, o processo falha; caso contrário, segue normalmente.

Com a chave pública do remetente, a assinatura digital é confirmada e por fim, o conteúdo é salvo no formato original e uma mensagem de sucesso é exibida para o usuário.

2.3.1.5 REGISTRO DE *LOGS*

A fim de possibilitar a auditoria ou rastreamento das atividades realizadas pela ferramenta, foi inserida também uma função que armazena todos os registros em um arquivo nomeado “security_log.txt”.

2.4 DISCUSSÃO DOS RESULTADOS

Os testes da ferramenta evidenciaram uma boa aceitação das suas funcionalidades. A interface possibilitou rápida e fácil comunicação com o usuário e os requisitos de segurança foram atendidos,

O programa foi disponibilizado para usuários de um grupo de controle específico que a empregaram para cifrar arquivos de variados formatos e tamanhos.

A aliança dos dois tipos de criptografia, simétrica e assimétrica, permitiu a robustez da codificação e a eficiência no processamento dos dados, resultando em uma aplicação que pode ser aplicada em diferentes cenários operacionais.

3. CONCLUSÃO

Este *script* foi projetado para ser uma ferramenta prática e segura para criptografia de arquivos, utilizando algoritmos robustos como AES e RSA. Cada etapa do processo é cuidadosamente organizada para garantir que os dados estejam protegidos durante todo o ciclo de vida, desde a geração das chaves até a criptografia e descriptografia dos arquivos.

3.1 RESULTADOS

A interface gráfica simples permite que qualquer usuário, independentemente do nível de conhecimento técnico, possa usar a ferramenta com facilidade.

O desenvolvimento deste *script* foi motivado pela necessidade de criar uma solução que possa atender aos desafios de Segurança Cibernética enfrentados em ambientes sensíveis, como Centros de Comando e Controle do Exército Brasileiro ou demais órgãos de Comunicações.

A principal preocupação é a manutenção da confidencialidade, da integridade e da autenticidade dos dados, evitando que informações sensíveis sejam acessadas ou modificadas por agentes não autorizados.

Nesse contexto, a ferramenta de criptografia desenvolvida tem como objetivo garantir a segurança das comunicações e do armazenamento de dados de forma eficiente e prática, mesmo para usuários que não possuem conhecimento técnico avançado.

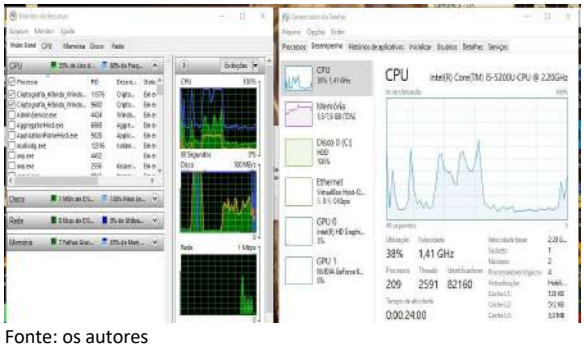
3.2 DESEMPENHO

Com a finalidade de avaliar o desempenho da ferramenta desenvolvida, foi utilizado um computador com as seguintes características: Sistema Operacional Windows 64, CPU i5 (5ª geração) e 8GB de memória RAM, com os resultados conforme tabela e figuras abaixo:

TABELA 5 – Primeira rodada de testes

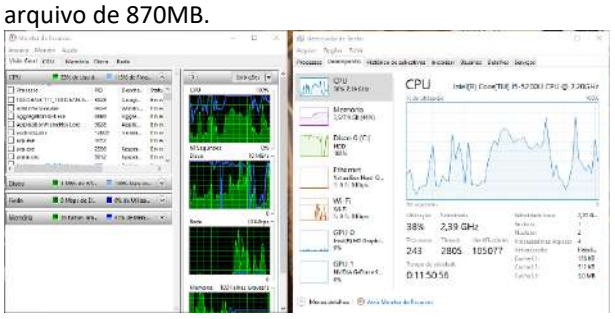
Tamanho do arquivo a ser cifrado	Tempo para cifrar	Tempo para decifrar
175MB	8 segundos	5 segundos
870 MB	50 segundos	30 segundos

FIGURA 5- Processamento durante a criptografia do arquivo de 870MB.



Fonte: os autores

FIGURA 6- Processamento durante a descriptografia do arquivo de 870MB.



Fonte: os autores.

Testes semelhantes foram realizados em outro computador de características semelhantes, porém com um processador i5 de 13ª geração. Os resultados se deram conforme abaixo:

TABELA 6 – Segunda rodada de testes

Tamanho do arquivo a ser cifrado	Tempo para cifrar	Tempo para decifrar
100MB	17 segundos	32 segundos
775MB	23 segundos	35 segundos

FIGURA 7 – Processamento durante a criptografia do arquivo de 100MB.

Fonte: os autores.

FIGURA 8 - Processamento durante a descriptografia do arquivo de 100MB.

Fonte: os autores.

A ferramenta mostrou-se eficiente tanto na sua funcionalidade quanto no tempo de execução. As variações do funcionamento entre as máquinas foram percebidas dentro de uma margem aceitável.

3.3 TESTES DE SEGURANÇA

Além da avaliação do desempenho da aplicação, outro exame necessário é o da validade dos arquivos de chaves gerados pelo programa. Esta verificação de integridade permite a correta execução da ferramenta sem comprometimento da segurança.

Com o comando *openssl*, pode-se verificar se a chave está no formato correto e não corrompida, evitando falhas na operação.

FIGURA 8 - Teste de validação da chave privada**.**

Fonte: os autores.

Também é possível checar as informações e propriedades do arquivo de chave, garantindo que ele está pronto para uso.

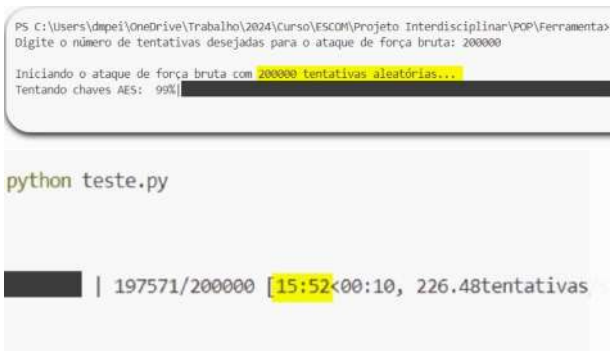
FIGURA 9 - Teste de validação da chave pública

Fonte: os autores.

A robustez da criptografia implementada na aplicação praticamente inviabiliza que os computadores mais avançados atualmente consigam tentar todas as combinações possíveis contra os algoritmos.

Executando um programa para realizar ataques de força bruta, foram determinadas 200.000 tentativas, as quais levaram cerca de 16 minutos para serem concluídas, sem sucesso.

FIGURA 9 – Ataque de força bruta
Fonte: os autores



Fonte: os autores.

Calcula-se, portanto, que para testar todas as combinações possíveis para quebrar um algoritmo AES-256, seriam necessários 1,65 x 10^59 anos.

Escalando a capacidade para um computador que possa realizar, por exemplo, 20 milhões de tentativas por segundo, o tempo médio cai para 1,835 x 10^51 anos, um número ainda inviável.

3.4 IMPLICAÇÕES PRÁTICAS E TEÓRICAS

Buscando conjugar elementos dos dois principais tipos de criptografia, a ferramenta desenvolvida trabalha com um modelo híbrido.

Dessa forma, é possível a transmissão de grandes quantidades de dados com segurança e eficiência, já que a funcionalidade simétrica garante boa velocidade na transmissão e a assimétrica protege a chave sem expô-la.

A obrigação de o usuário fornecer uma senha implementa também a autenticação de dois fatores, sendo um deles algo que o usuário tem (chave) e o outro algo que ele sabe (senha).

3.5 LIMITAÇÕES E CONSIDERAÇÕES

Embora a aplicação procure o melhor resultado ao combinar os algoritmos de ambos os tipos de criptografia, ainda é possível que a comunicação fique exposta a alguns riscos.

Ainda que as chaves estejam protegidas, a possível ausência de um canal de transmissão seguro entre os usuários, pode acarretar na interceptação das mesmas.

Se o usuário não inserir uma senha forte durante sua execução, ataques de força bruta podem ser suficientes para decodificá-la. Bem como, ela pode ser obtida por meio de técnicas de engenharia social.

Quanto ao seu funcionamento, apesar da sua boa execução, o programa não demonstra muita flexibilidade ao salvar todos os arquivos gerados no mesmo diretório local do executável. Futuras versões podem mitigar essa restrição.

3.6 RECOMENDAÇÕES FUTURAS

Os conhecimentos sobre a Segurança da Informação e a Proteção Cibernética estão sujeitos à constante revisão. Uma vez que a tecnologia segue evoluindo e novas ameaças são desenvolvidas, é crucial que o programa seja continuamente testado e sofra as devidas atualizações que se fizerem necessárias para garantir a inviolabilidade dos dados por ele protegidos.

Da mesma forma, é interessante que além de atualizada, a ferramenta possa ser integrada a outros sistemas utilizados pela Força Terrestre, inclusive com acesso à EBNet a fim de estabelecer um canal de comunicação seguro entre as partes.

ABSTRACT

This work aims to provide informations that can contribute to the development of data encryption and decryption application for the needs of the Brazilian Army's operations. Based on a summary analysis of the existing literature on the subject, the requirements for the development of a program that will implement encryption and decryption algorithms in a graphical interface will be defined, ensuring

security, performance and simplicity so that the user can protect his information from the various current cyber threats, in a efficient and safe way.

5 REFERÊNCIAS

BONEH, Dan. *Twenty Years of Attacks on the RSA Cryptosystem.* Notices of the American Mathematical Society, v. 46, n. 2, 1999.

DAEMEN, Joan; RIJMEN, Vincent. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Berlim: Springer-Verlag, 2001.

DIFFIE, Whitfield; LANDAU, Susan. *Privacy on the line: the politics of wiretapping and encryption*. Massachusetts: The MIT Press, 2007.

EXÉRCITO BRASILEIRO. *Doutrina Militar de Defesa Cibernética* (MD31-M-07). Brasília, 2023.

EXÉRCITO BRASILEIRO. *Diretriz Estratégica Organizadora do Sistema de Comando e Controle do Exército* (EB10-D-01.013). Brasília, 2021.

EXÉRCITO BRASILEIRO. *Manual de Guerra Cibernética* (EB70-MC-10.232). Brasília, 2017.

FERGUSON, Neil; SCHNEIER, Bruce; KOHNO, Tadayoshi. *Cryptography Engineering: Design Principles and Practice Applications*. New York: Wiley, 2010.

INTERNET ENGINEERING TASK FORCE (IETF). *RFC 1321: The MD5 message-digest algorithm*. Disponível em <https://www.ietf.org/rfc/rfc1321.txt> Acesso em: 28 out. 2024.

HELLMAN, Martin E. *An overview of public key cryptograph*. IEEE Communications Magazine, v. 16, n. 6, 1978.

KATZ, Jonathan; LINDELL, Yehuda. *Introduction to Modern Cryptography*. Boca Raton: CRC Press, 2007.

MENEZES, Alfred J.; VAN OORSCHOT, Paul C.; VANSTONE, Scott A. *Handbook of Applied Cryptography.* Boca Raton: CRC Press, 1996.

NAKAMURA, Emílio Tissato. GEUS, Paulo Lício de. Segurança de Redes em Ambientes Corporativos. São Paulo: Novatec Editora, 2007.

PAAR, Christof; PELZL, Jan. *Understanding Cryptography: A Textbook for Students and Practitioners.* Berlim: Springer-Verlag, 2010

SCHNEIER, Bruce. *Applied Cryptography*. New York: Wiley, 1996.

STALLINGS, William. *Criptografia e segurança de redes: Princípios e práticas*. São Paulo: Editora Pearson, 2015.

TANENBAUM, Andrew S. *Redes de computadores*. São Paulo: Editora Pearson Prentice Hall, 2011.

Brasília - DF, 8 de novembro de 2024.

RAPHAEL MACHADO DA SILVA RODRIGUES – Maj
Chefe da Seção de Ensino de TIC e Prot Ciber

APÊNDICE A – CONFECÇÃO E OPERAÇÃO DE UM PROGRAMA DE CRIPTOGRAFIA DE DADOS: PROCEDIMENTO OPERACIONAL PADRÃO (POP)

DESENVOLVIMENTO DE UMA FERRAMENTA DE CRIPTOGRAFIA DE DADOS: PRODUÇÃO DE UMA FERRAMENTA DE CRIPTOGRAFIA E DESCRIPTOGRAFIA PARA PROTEÇÃO DE DADOS ATRAVÉS DE UMA INTERFACE GRÁFICA

Cap **Flávio** Barros Correia
Cap Diego Madureira **Peixoto**
Cap Cassius Matheus Alves **Bierhals**

A.1 OBJETIVO

A.1.1 Fornecer diretrizes para a confecção, configuração e operação de um programa de criptografia de dados, incluindo instruções para o desenvolvimento e uso de um script de criptografia de dados, bem como padronizar o processo de utilização dele, garantindo a integridade, confidencialidade e disponibilidade das informações trocadas entre sistemas e unidades militares. Esse procedimento visa proporcionar uma camada de segurança adicional para prevenir acessos não autorizados e assegurar que as comunicações sejam protegidas contra ameaças cibernéticas durante operações.

A.2 ÁREA OU SETOR RESPONSÁVEL

A.2.1 Departamento de Tecnologia da Informação (TI).

A.3 REFERÊNCIAS

A.3.1 Documentação oficial da biblioteca PyCryptodome (https://pycryptodome.readthedocs.io/en/latest/src/api.html); e
A.3.2 Manual de Campanha EB70-MC-10.232 Guerra Cibernética, 1ª Edição, 2017.

A.4 MATERIAIS E EQUIPAMENTOS NECESSÁRIOS

A.4.1 Hardware compatível para servidor e estações de trabalho, com capacidade suficiente para processar operações de criptografia.
A.4.2 Python e as bibliotecas PyCryptodome para criptografia e Tkinter para interface gráfica.
A.4.3 Acesso à internet para atualização de bibliotecas e consulta de documentação online, se necessário.
A.4.4 Documentação técnica sobre criptografia, contendo especificações de segurança e manuais de referência para configuração e operação segura.
A.4.6 Ferramentas de backup e recuperação de dados para garantir a integridade e a disponibilidade das informações em caso de falha no sistema.

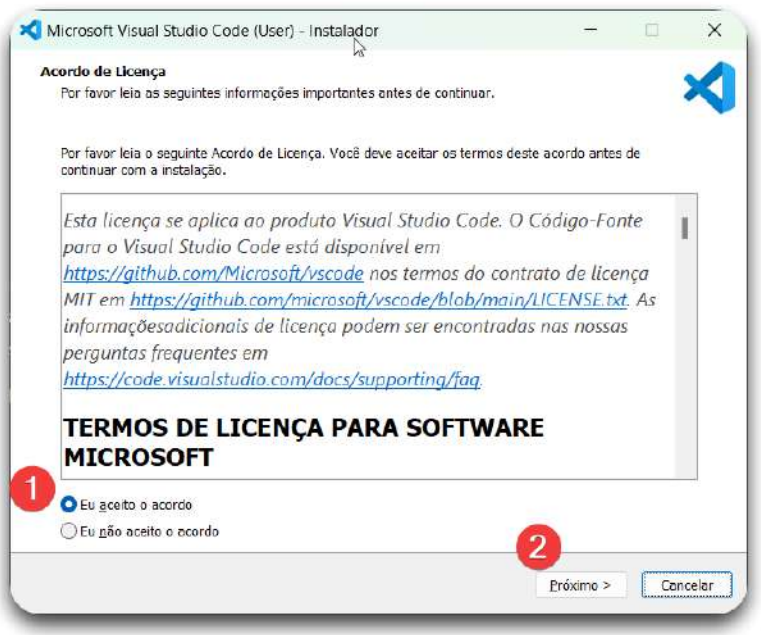
A.5 PROCEDIMENTOS PASSO A PASSO

A.5.1 INSTALAÇÃO

A.5.1.1 Preparação do Ambiente

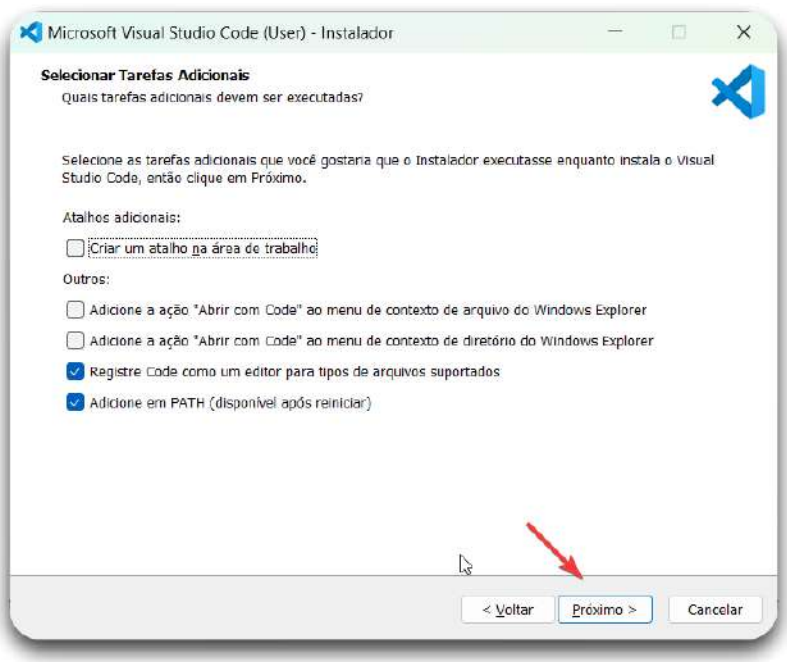
A.5.1.1.1: Para melhor visualização do código e por ocasião deste POP, será utilizado o editor de código fonte Visual Studio Code (https://code.visualstudio.com/download)

FIGURA 1 – Passo 1 da instalação do programa



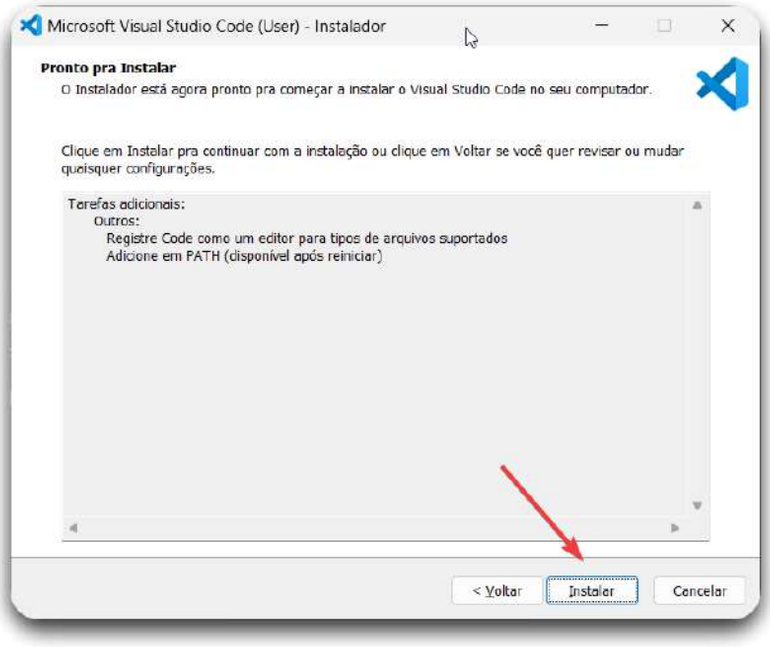
Fonte: os autores.

FIGURA 2 - Passo 2 da instalação do programa



Fonte: os autores.

FIGURA 3 - Passo 3 da instalação do programa



Fonte: os autores.

DESCRIÇÃO DO PASSO: *Para instalar o Visual Studio Code, aceite o acordo de licença e clique em "Próximo". Marque as opções desejadas, incluindo criar um atalho e adicionar ao PATH, e clique em "Próximo". Confirme as configurações e clique em "Instalar" para iniciar.*
No Linux também pode ser baixado via terminal através do comando: sudo apt update && sudo apt install code.

A.5.1.1.2 Instalar o Python, que será a linguagem de programação utilizada para a confecção do script de criptografia (https://www.python.org/downloads/)

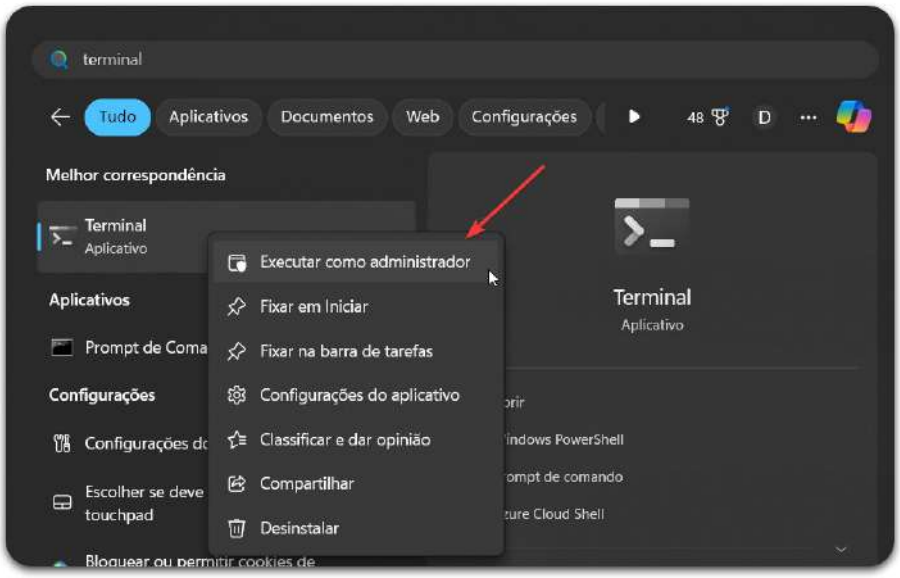
FIGURA 4 – Instalação do Python

Fonte: os autores

DESCRIÇÃO DO PASSO: *Para instalar o Python, marque a opção "Use admin privileges when installing py.exe" para garantir permissões administrativas e "Add python.exe to PATH" para adicionar o Python ao PATH do sistema. Em seguida, clique em "Install Now" para iniciar a instalação com as configurações padrão.*
No Linux, a instalação do Python pode ser feita diretamente pelo terminal. Use os seguintes comandos: sudo apt update && sudo apt install python3

A.5.1.1.3 Instalação das bibliotecas de python necessárias para confecção do script:

FIGURA 5 – Instalação das bibliotecas



Fonte: os autores

DESCRIÇÃO DO PASSO: Abra o terminal e execute: no Windows, ***pip install pycryptodome pyinstaller*** *(*o Tkinter já vem com o Python); no Linux, ***pip install pycryptodome pyinstaller*** e ***sudo apt-get install python3-tk***

A.5.2 CONFECÇÃO DO SCRIPT

A.5.2.1 Script de Criptografia Híbrida

A.5.2.1.1 Dentro do Visual Studio Code, crie um arquivo "***.py***" onde será inserido o script para criptografia híbrida. O script completo será disponibilizado no final do pop:

FIGURA 6 – Trecho do script

```
from tkinter import Tk, Label, Button, filedialog, messagebox, simpledialog
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP, AES
from Crypto.Random import get_random_bytes
from Crypto.Hash import SHA256
from Crypto.Signature import pkcs1_15
import base64
import os
from datetime import datetime
```

Fonte: os autores

DESCRIÇÃO DO PASSO: Primeiramente serão realizadas as importações de bibliotecas essenciais para o funcionamento do script de criptografia. O ***tkinter*** fornece componentes de interface gráfica, como botões e caixas de diálogo. A biblioteca ***Crypto*** (do pacote PyCryptodome) importa módulos para geração e uso de chaves RSA, criptografia AES, geração de bytes aleatórios, e criação de hashes e assinaturas digitais. ***base64*** é usada para codificação de dados, ***os*** para operações no sistema, e ***datetime*** para registros de data e hora em logs ou relatórios.

A.5.2.1.2 Funções de utilidade dentro no script de criptografia:

FIGURA 7 – Funções de utilidade

```
def log_action(action, status, file_path=""):
    with open("security_log.txt", "a") as log_file:
        log_file.write(f"[{datetime.now()}] - {action}: {status} - {file_path}\n")

def show_message(success, msg, action="", file_path=""):
    if success:
        messagebox.showinfo("Sucesso", msg)
    else:
        messagebox.showerror("Erro", msg)
    log_action(action, "Sucesso" if success else "Falha", file_path)

def prompt_password(prompt_text="Digite a senha:"):
    return simpledialog.askstring("Senha", prompt_text, show='*')

def load_key(file_path, key_type):
    try:
        with open(file_path, "rb") as key_file:
            key_data = key_file.read()
            if key_type == "private":
                password = prompt_password("Digite a senha da chave privada:")
                if not password:
                    raise ValueError("Senha não fornecida.")
                key = RSA.import_key(key_data, passphrase=password)
            else:
                key = RSA.import_key(key_data)
            if key_type == "public" and key.has_private():
                raise ValueError("Esperava chave pública, mas uma chave privada foi fornecida.")
            if key_type == "private" and not key.has_private():
                raise ValueError("Esperava chave privada, mas uma chave pública foi fornecida.")
            return key
    except Exception as e:
        show_message(False, f"Erro ao carregar chave {key_type}: {e}", f"Carregar chave {key_type}", file_path)
        return None
```

Fonte: os autores

DESCRIÇÃO DO PASSO: Essas funções de utilidade ajudam no gerenciamento do script. A função ***log_action*** registra as ações em um arquivo de log com data e hora; ***show_message*** exibe mensagens de sucesso ou erro para o usuário e registra a ação; ***prompt_password*** solicita uma senha ao usuário; e ***load_key*** carrega uma chave RSA (privada ou pública) do arquivo, pedindo senha se necessário e verificando se o tipo de chave está correto, garantindo segurança e usabilidade.

A.5.2.1.3 Função para gerar as chaves RSA:

FIGURA 8 – Função generate_rsa_keys()

```
def generate_rsa_keys():
    try:
        # Pedir o nome da chave
        key_name = simpledialog.askstring("Nome da Chave", "Escolha um nome para as chaves RSA:")
        if not key_name:
            show_message(False, "Nome da chave não pode estar vazio.", "Gerar chave RSA")
            return

        password = None
        while True:
            password = prompt_password("Digite uma senha para proteger a chave privada:")
            if password:
                confirm_password = prompt_password("Confirme a senha:")
                if password == confirm_password:
                    break
                else:
                    show_message(False, "As senhas não coincidem. Tente novamente.", "Gerar chave RSA")
            else:
                show_message(False, "Senha não pode estar vazia. Tente novamente.", "Gerar chave RSA")

        # Gerar as chaves RSA
        key = RSA.generate(4096)
        private_key_filename = f"{key_name}_priv.pem"
        public_key_filename = f"{key_name}_pub.pem"

        with open(private_key_filename, "wb") as priv_file, open(public_key_filename, "wb") as pub_file:
            priv_file.write(key.export_key(passphrase=password, pkcs=8, protection="scryptAndAES128-CBC"))
            pub_file.write(key.publickey().export_key())

        show_message(True, f"Chaves RSA geradas e salvas como {private_key_filename} e {public_key_filename}.", "Gerar chave RSA")
    except Exception as e:
        show_message(False, f"Erro ao gerar chaves RSA: {e}", "Gerar chave RSA")
```

Fonte: os autores

DESCRIÇÃO DO PASSO: A função ***generate_rsa_keys*** cria um par de chaves RSA (privada e pública). Primeiro, pede ao usuário um nome para as chaves e uma senha para proteger a chave privada. A senha é confirmada para garantir precisão. As chaves são geradas com 4096 bits e salvas em arquivos com nomes baseados na escolha do usuário. Em caso de sucesso ou erro, uma mensagem é exibida ao usuário, informando o resultado da operação.

A.5.2.1.4 Função para criptografia:

FIGURA 9 – Função encrypt_file()

```
def encrypt_file(public_key_path, private_key_path, file_path):
    try:
        public_key = load_key(public_key_path, "public")
        private_key = load_key(private_key_path, "private")
        if not public_key or not private_key:
            return

        aes_key = get_random_bytes(32)
        with open(file_path, "rb") as f:
            file_data = f.read()

        cipher_aes = AES.new(aes_key, AES.MODE_GCM)
        ciphertext, tag = cipher_aes.encrypt_and_digest(file_data)
        encrypted_aes_key = PKCS1_OAEP.new(public_key).encrypt(aes_key)
        signature = pkcs1_15.new(private_key).sign(SHA256.new(ciphertext))

        with open(f"{file_path}.enc", "wb") as enc_file:
            for item in [cipher_aes.nonce, encrypted_aes_key, ciphertext, tag, signature, os.path.splitext(file_path)[1].encode()]:
                enc_file.write(base64.b64encode(item) + b'\n')

        show_message(True, f"Arquivo '{file_path}' criptografado com sucesso.", "Criptografar arquivo", file_path)

    except Exception as e:
        show_message(False, f"Erro durante a criptografia: {e}", "Criptografar arquivo", file_path)
```

Fonte: os autores

DESCRIÇÃO DO PASSO: A função ***encrypt_file*** criptografa um arquivo usando uma chave AES gerada aleatoriamente e criptografa essa chave AES com a chave pública RSA. Ela também gera uma assinatura digital com a chave privada RSA para garantir a integridade. O arquivo criptografado é salvo com extensão ***.enc*** e inclui a chave AES criptografada, o texto cifrado, a tag de autenticação, a assinatura e a extensão original do arquivo. Em caso de sucesso ou erro, uma mensagem é exibida ao usuário com o status da operação.

A.5.2.1.5 Função para descriptografia:

FIGURA 10 – Função decrypt_file()

```
def decrypt_file(public_key_path, private_key_path, file_path):
    try:
        public_key = load_key(public_key_path, "public")
        private_key = load_key(private_key_path, "private")
        if not public_key or not private_key:
            return

        with open(file_path, "rb") as enc_file:
            nonce, encrypted_aes_key, ciphertext, tag, signature, file_extension = [base64.b64decode(enc_file.readline().strip()) for _ in range(6)]

        aes_key = PKCS1_OAEP.new(private_key).decrypt(encrypted_aes_key)
        cipher_aes = AES.new(aes_key, AES.MODE_GCM, nonce=nonce)
        decrypted_data = cipher_aes.decrypt_and_verify(ciphertext, tag)
        pkcs1_15.new(public_key).verify(SHA256.new(ciphertext), signature)

        output_file_path = filedialog.asksaveasfilename(title="Salvar arquivo descriptografado como", defaultextension=file_extension.decode())
        if output_file_path:
            with open(output_file_path, "wb") as out_file:
                out_file.write(decrypted_data)
            show_message(True, f"Arquivo '{output_file_path}' descriptografado com sucesso.", "Descriptografar arquivo", output_file_path)

    except Exception as e:
        show_message(False, f"Erro durante a descriptografia: {e}", "Descriptografar arquivo", file_path)
```

Fonte: os autores

DESCRIÇÃO DO PASSO: A função ***decrypt_file*** descriptografa um arquivo usando a chave privada RSA para recuperar a chave AES e, em seguida, descriptografa o conteúdo do arquivo com AES. Ela também verifica a assinatura digital com a chave pública para assegurar a integridade do arquivo. Após a descriptografia, o usuário escolhe onde salvar o arquivo restaurado com sua extensão original. Em caso de sucesso ou erro, uma mensagem informa o status da operação ao usuário.

A.5.2.1.6 Funções para interface gráfica:

FIGURA 11 – Funções para interface gráfica

```
def encrypt_file_ui():
    public_key = filedialog.askopenfilename(title="Selecione a chave pública do destinatário", filetypes=[("Chave Pública", "*.pem")])
    private_key = filedialog.askopenfilename(title="Selecione a sua chave privada", filetypes=[("Chave Privada", "*.pem")])
    file_path = filedialog.askopenfilename(title="Selecione o arquivo para criptografar", filetypes=[("Todos os arquivos", "*.*")])
    if public_key and private_key and file_path:
        encrypt_file(public_key, private_key, file_path)

def decrypt_file_ui():
    private_key = filedialog.askopenfilename(title="Selecione a sua chave privada", filetypes=[("Chave Privada", "*.pem")])
    public_key = filedialog.askopenfilename(title="Selecione a chave pública do remetente", filetypes=[("Chave Pública", "*.pem")])
    encrypted_file = filedialog.askopenfilename(title="Selecione o arquivo criptografado", filetypes=[("Arquivo Criptografado", "*.enc")])
    if private_key and public_key and encrypted_file:
        decrypt_file(public_key, private_key, encrypted_file)

def create_gui():
    root = Tk()
    root.title("Criptografia de Arquivos")
    Label(root, text="Escolha uma operação:", font=("Arial", 14)).pack(pady=10)
    Button(root, text="Gerar Chaves RSA", command=generate_rsa_keys, width=25).pack(pady=5)
    Button(root, text="Criptografar Arquivo", command=encrypt_file_ui, width=25).pack(pady=5)
    Button(root, text="Descriptografar Arquivo", command=decrypt_file_ui, width=25).pack(pady=5)
    root.geometry("300x200")
    root.mainloop()
```

Fonte: os autores

DESCRIÇÃO DO PASSO: Essas funções criam a interface gráfica para criptografia de arquivos. ***encrypt_file_ui*** e ***decrypt_file_ui*** permitem que o usuário selecione as chaves e o arquivo para criptografar ou descriptografar usando caixas de diálogo. A função ***create_gui*** configura a janela principal com botões para gerar chaves RSA, criptografar e descriptografar arquivos, tornando o processo acessível e fácil de usar.

A.5.2.1.7 Função para execução do programa:

FIGURA 12 – Função principal

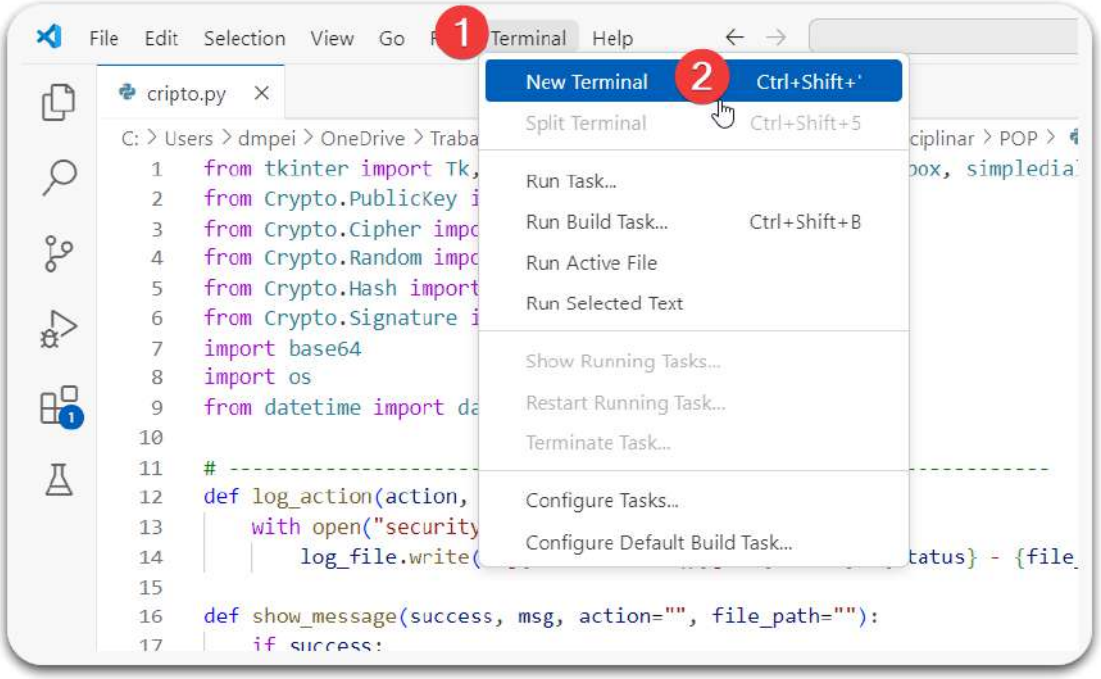
```
if __name__ == "__main__":
    create_gui()  # Inicia a interface gráfica
```

Fonte: os autores

DESCRIÇÃO DO PASSO: A condição ***if __name__ == "__main__"***: verifica se o script está sendo executado diretamente. Se for o caso, a função ***create_gui()*** é chamada, iniciando a interface gráfica do usuário para acessar as funcionalidades de criptografia e descriptografia de arquivos.

A.5.2.1.8 Importando o script em um executável:

FIGURA 13 – Passo 1 da importação do script



Fonte: os autores

FIGURA 12 - Passo 2 da importação do script

Fonte: os autores

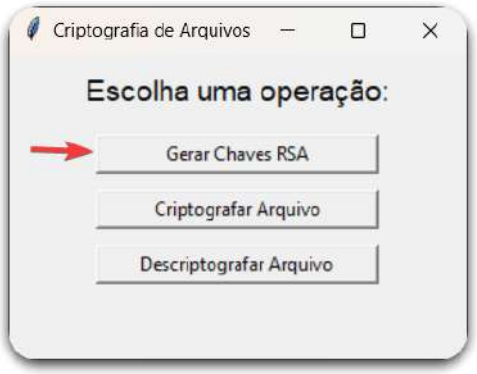
DESCRIÇÃO DO PASSO: Para exportar o script como executável no Visual Studio Code, abra o terminal integrado, navegue até o diretório do script e execute ***pyinstaller --onefile --windowed nome_do_script.py*** no terminal. O executável será gerado na pasta ***dist*** dentro do diretório do projeto, pronto para uso sem necessidade de um ambiente Python.
Nota: O executável gerado pelo PyInstaller funcionará apenas no sistema operacional onde o comando foi executado. Para criar versões para Windows e Linux, é necessário rodar o comando em cada sistema operacional.

A.5.3 OPERAÇÃO

A.5.3.1 Gerando Chaves RSA

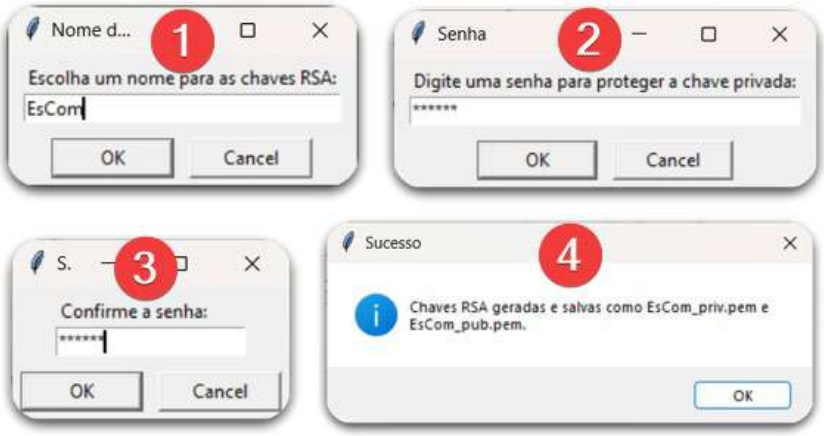
A.5.3.1.1 Gerar as chaves públicas e privadas que irão servir para garantir a integridade e autenticidade dos dados:

FIGURA 13 – Seleção da opção “gerar chaves RSA” no programa



Fonte: os autores.

FIGURA 14 - Passo a passo da geração de chaves



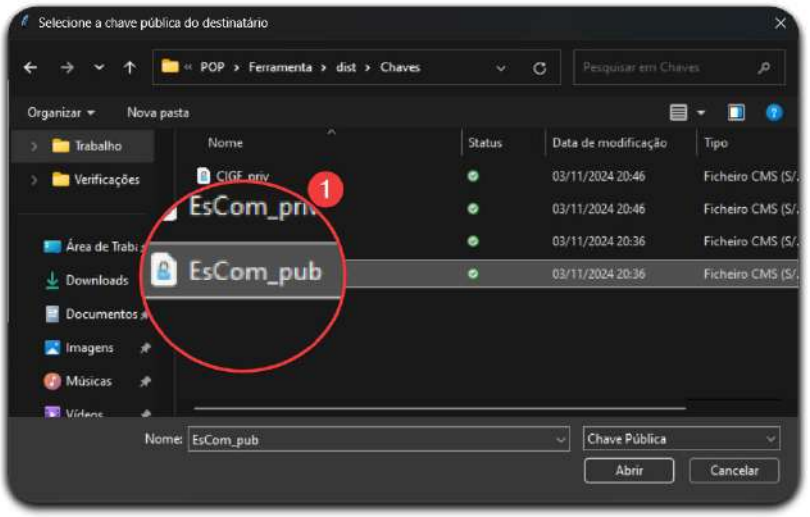
Fonte: os autores.

DESCRIÇÃO DO PASSO: Clique em "***Gerar Chaves RSA***", insira um nome para o par de chaves e defina uma senha para proteger a chave privada, confirmando-a em seguida. As chaves serão salvas na mesma pasta do programa com os nomes escolhidos (***ex: EsCom_priv.pem e EsCom_pub.pem***).

A.5.3.2 Criptografando arquivos

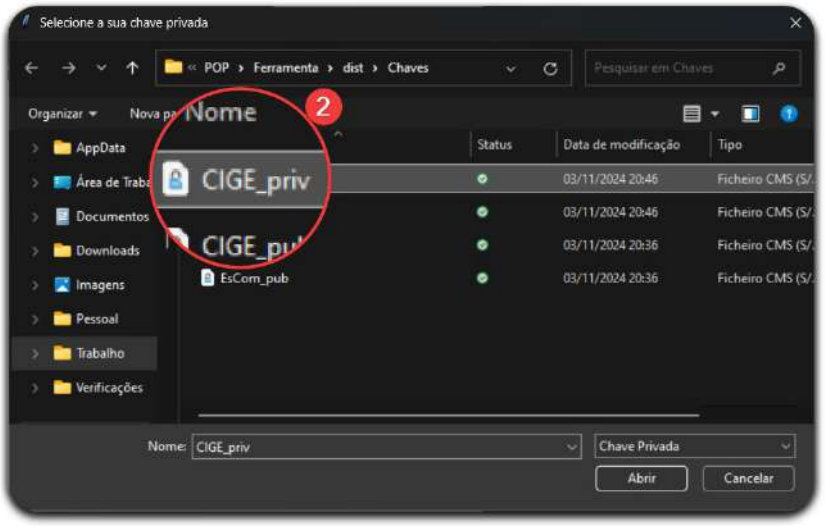
A.5.3.2.1 Este passo utiliza criptografia para proteger o arquivo selecionado com as chaves RSA;

FIGURA 15 – Seleção da chave pública



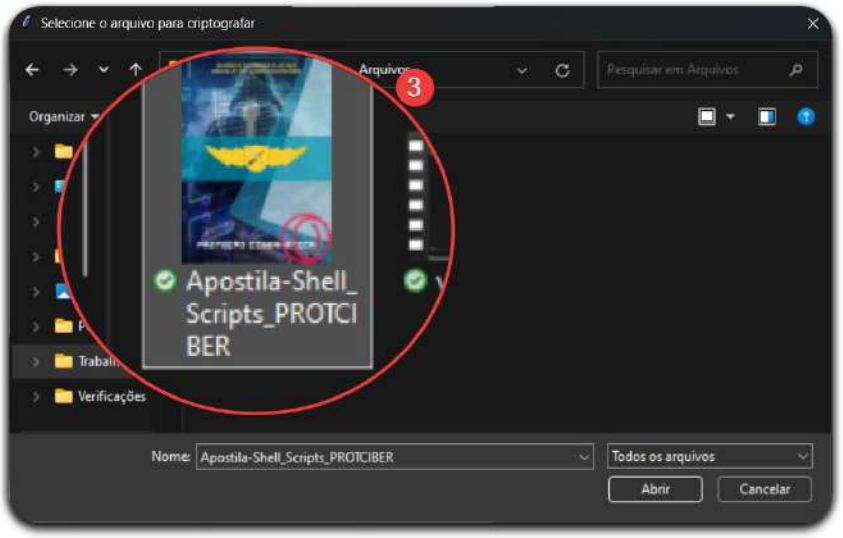
Fonte: os autores.

FIGURA 16 - Seleção da chave privada



Fonte: os autores.

FIGURA 17 - Seleção do arquivo a ser cifrado



Fonte: os autores.

FIGURA 18 – Digitação da senha e mensagem final

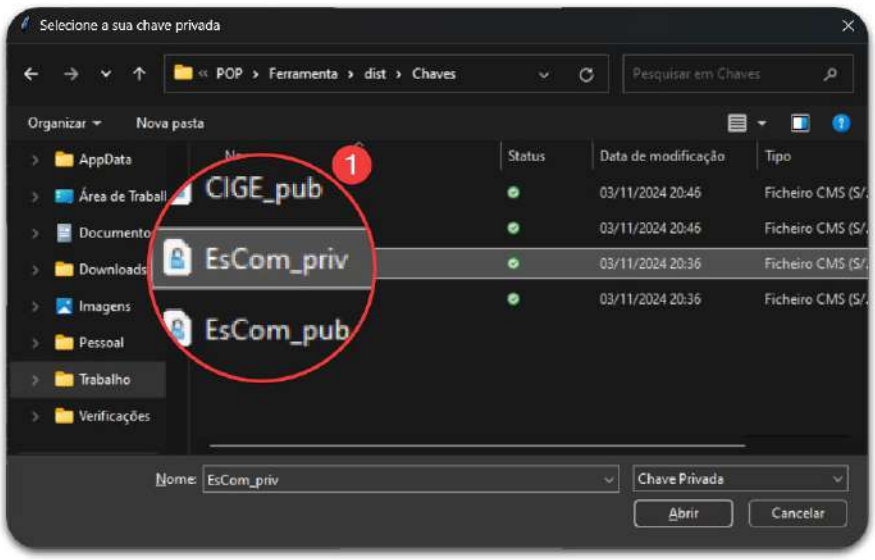
Fonte: os autores.

DESCRIÇÃO DO PASSO: Para criptografar um arquivo, clique em "***Criptografar Arquivo***" e selecione a chave pública do destinatário (***EsCom_pub.pem***). Em seguida, escolha sua chave privada (***CIGE_priv.pem***) e o arquivo que deseja criptografar. Insira a senha da chave privada quando solicitado. Ao final, uma mensagem de sucesso confirmará que o arquivo foi criptografado, e a versão criptografada será salva na mesma pasta do arquivo original, com a extensão "***. enc***".

A.5.3.3 Descriptografando arquivos

A.5.3.2.1 Este passo reverte a criptografia, restaurando o arquivo original.;

FIGURA 19 – Seleção da chave privada

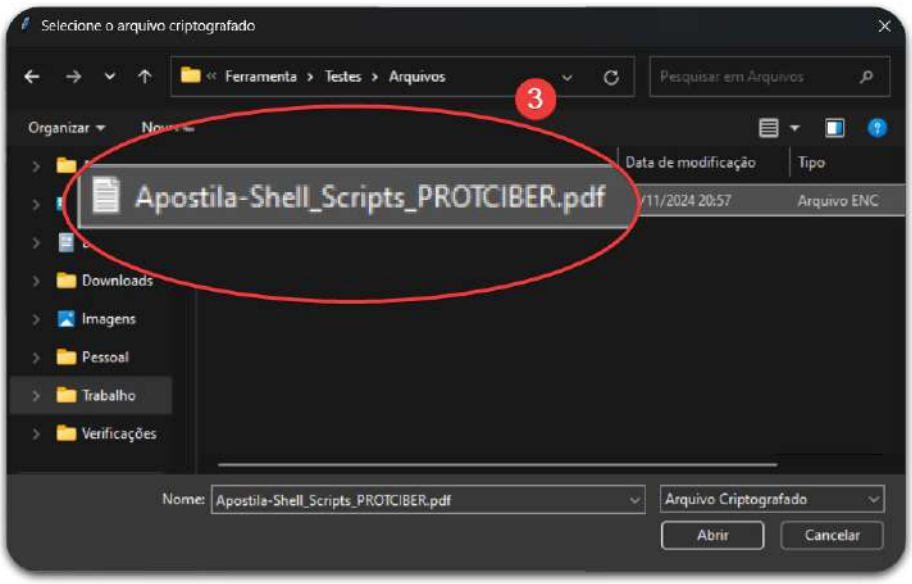


Fonte: os autores.

FIGURA 20 - Seleção da chave pública

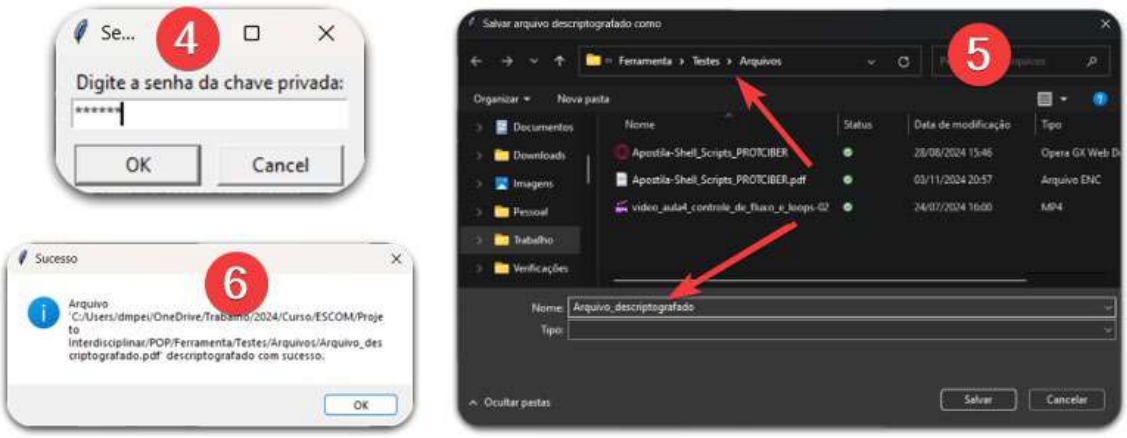
Fonte: os autores.

FIGURA 21 - Seleção do arquivo a ser decifrado



Fonte: os autores.

FIGURA 22 - Digitação da senha e mensagem final



Fonte: os autores.

DESCRIÇÃO DO PASSO: Para descriptografar um arquivo, clique em "***Descriptografar Arquivo***" e selecione sua chave privada (***EsCom_priv.pem***) e a chave pública do remetente (***CIGE_pub.pem***). Escolha o arquivo criptografado (tipo ***enc***) e, em seguida, insira a senha da chave privada quando solicitado. Defina o local e o nome para salvar o arquivo descriptografado e confirme. Uma mensagem de sucesso indicará que o arquivo foi restaurado com sucesso no local escolhido.

A.6 CONTROLES DE QUALIDADE

A.6.1 Realizar testes de criptografia e descriptografia após a geração das chaves e configuração para garantir que o programa está operando corretamente.

A.6.2 Verificar a integridade dos arquivos criptografados e descriptografados para assegurar que não houve perda de dados durante o processo.

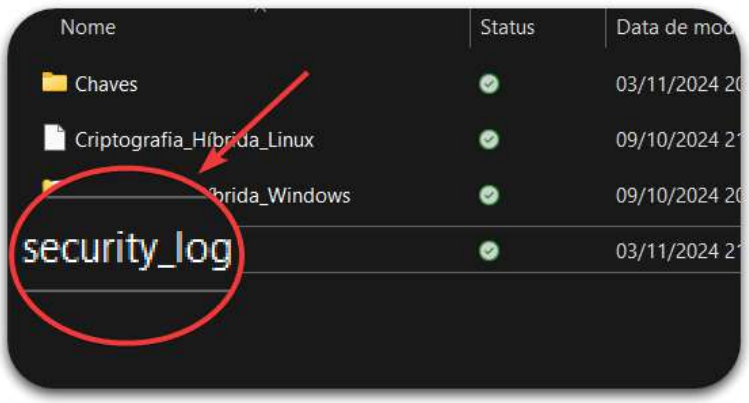
A.6.3 Realizar testes de compatibilidade das chaves RSA, assegurando que somente a chave privada correspondente pode descriptografar os arquivos.

A.6.4 Testar a interface gráfica para garantir que todas as funcionalidades (geração de chaves, criptografia, descriptografia) estão operando sem erros.

A.7 REGISTROS E DOCUMENTAÇÃO

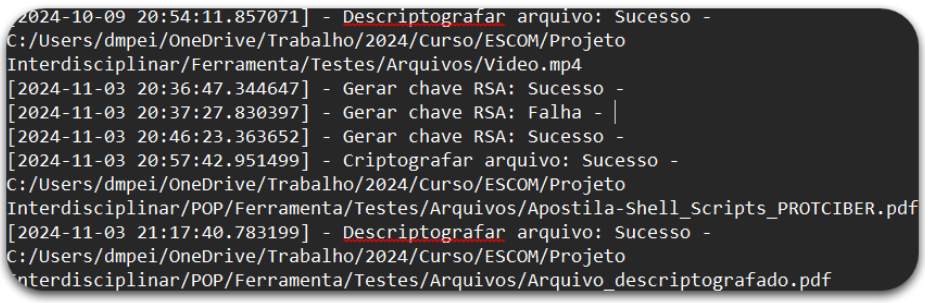
A.7.1 Manter registros de todas as etapas do processo de geração de chaves, criptografia e descriptografia de arquivos e documentar qualquer problema encontrado durante o uso do programa, como falhas na criptografia ou erros de autenticação.

FIGURA 23 – Arquivo de log gerado



Fonte: os autores.

FIGURA 24 – Conteúdo do arquivo de log



Fonte: os autores.

DESCRIÇÃO DO PASSO: O log do programa, criado automaticamente no arquivo security_log.txt na mesma pasta onde o programa é executado, registra todas as ações realizadas, como geração de chaves, operações de criptografia e descriptografia, além de eventuais falhas. Cada entrada inclui a data, a ação executada, o status (sucesso ou falha) e, quando aplicável, o caminho do arquivo envolvido.

A.8 RESPONSABILIDADES

A.8.1 O responsável pela TI é responsável por supervisionar a implementação do programa de acordo com este POP; e

A.8.2 Os usuários finais são responsáveis por reportar quaisquer problemas ou necessidades de suporte relacionadas ao uso do programa de criptografia híbrida.

A.9 ANEXOS

A.9.1 Script do programa completo, em formato .py

UTILIZAÇÃO DE RASPBERRY COMO GATEWAY DE ANONIMIZAÇÃO

S Ten Marcio **Da Silveira** Pinto
Sgt Lucas Pimentel **Diniz**

RESUMO

Neste século XXI viu-se uma expansão dos meios de tecnologia da informação. Tamanho foi este crescimento, que por muitas vezes o mundo digital se confunde com o real. As pessoas adotam um estilo de vida digital para várias rotinas e ações em seu dia a dia. Um exemplo está em como lidamos com nossas operações financeiras. Qualquer que seja a necessidade, não há mais a obrigatoriedade de irmos a uma agência fisica. Uma vasta gama de situações são resolvidas através de um aplicativo na palma de nossas mãos. O que falar, então, de conceitos como Internet of Things (IoT), Cyber Intelligence, Threat Intelligence, Cloud Computing, dentre outros.

Palavras-chave: IOT , Gateway, Anonimização.

INTRODUÇÃO

No cenário atual, o avanço das tecnologias digitais tornou-se um elemento essencial para a vida cotidiana, impactando diretamente a forma como interagimos com o mundo ao nosso redor. Contudo, essa crescente interconectividade também trouxe consigo desafios significativos para a privacidade e segurança, questões que se tornam ainda mais críticas no contexto militar. À medida que as operações cibernéticas ganham relevância, a anonimização e a proteção de dados sensíveis tornam-se vitais para a segurança nacional e a eficácia das operações de inteligência.

Este artigo aborda a continuidade de um projeto que visa aprimorar o uso de gateways de anonimização em operações militares, utilizando dispositivos de baixo custo como o Raspberry Pi. Explorando soluções para instabilidade de data e hora, além da implementação de VPN over TOR, o trabalho busca garantir que operadores militares possam realizar suas missões com maior segurança e anonimato, sem a necessidade de expertise técnica. A pesquisa e desenvolvimento contínuos são fundamentais para alcançar um estado da arte nesse campo e fortalecer as capacidades operacionais do Exército Brasileiro.

1. DESENVOLVIMENTO

1.1 A INTERCONECTIVIDADE E A DEPENDÊNCIA TECNOLÓGICA

O avanço tecnológico nas últimas décadas transformou profundamente a maneira como a humanidade interage com o mundo ao seu redor. A interconectividade, que antes era um conceito distante, agora é uma realidade onipresente que molda todos os aspectos da vida moderna. Dispositivos conectados, como smartphones, computadores e dispositivos IoT, tornaram-se extensões das atividades diárias, proporcionando acesso imediato a informações, comunicação e serviços de todas as partes do mundo.

FIGURA 1 - Internet Of Everything

Fonte: (ALAMY,2016)

No entanto, essa transformação não veio sem custo. A dependência dessas tecnologias é tamanha que, sem elas, é difícil imaginar manter a mesma qualidade de vida. As comodidades digitais, como o acesso rápido a notícias, a capacidade de realizar transações financeiras online e a comunicação instantânea, tornaram-se indispensáveis. Essa dependência criou uma sociedade em que a privacidade e a segurança são frequentemente sacrificadas em troca de conveniência.

Os computadores e dispositivos móveis, que armazenam informações pessoais, revelam uma quantidade impressionante de detalhes sobre os indivíduos. Esses dados vão desde preferências de navegação até informações de localização, que podem ser usadas para inferir hábitos, interesses e até padrões de comportamento. Cada página da web visitada, cada aplicativo utilizado, potencialmente expõe informações sobre a localização geográfica do usuário, os locais que ele frequenta e até as redes sociais que ele utiliza. Essa exposição contínua torna evidente a fragilidade da privacidade no mundo digital.

Essa nova realidade impõe um desafio significativo: como equilibrar a interconectividade com a proteção da privacidade e da segurança? À medida que a dependência tecnológica cresce, a necessidade de desenvolver e implementar soluções robustas de segurança torna-se cada vez mais urgente. A sociedade moderna precisa repensar sua relação com a tecnologia, buscando formas de preservar a privacidade e a segurança sem abrir mão dos benefícios que a interconectividade proporciona.

1.2 A SEGURANÇA EM UM CENÁRIO DE GUERRA CIBERNÉTICA

O avanço da tecnologia não apenas alterou a vida cotidiana, mas também redefiniu o cenário de conflitos e guerras. O ciberespaço emergiu como um novo teatro de operações, onde as fronteiras físicas são irrelevantes, e os ataques cibernéticos podem ser lançados de qualquer lugar do mundo. Diferente das guerras convencionais, onde o poder militar é medido pela força física e pela capacidade de destruição, as guerras cibernéticas são travadas no campo da informação e da tecnologia.

Um ataque cibernético bem-sucedido pode causar danos que ultrapassam em muito os impactos de um ataque cinético. Imagine um cenário em que uma infraestrutura crítica, como uma rede elétrica ou um sistema de transporte, seja comprometida por um ataque cibernético. As consequências podem ser catastróficas, afetando milhões de pessoas, paralisando economias e desestabilizando governos. A capacidade de um ataque cibernético de atingir alvos específicos, com precisão e sem necessidade de proximidade física, torna essa forma de guerra extremamente perigosa.

Nesse novo cenário, as forças armadas precisam adaptar suas estratégias para enfrentar as ameaças digitais. A defesa cibernética tornou-se uma prioridade, exigindo que as forças militares desenvolvam capacidades avançadas para proteger suas redes e infraestruturas críticas. Além disso, é necessário que essas forças sejam capazes de identificar e neutralizar ameaças cibernéticas antes que causem danos irreversíveis.

Para isso, a produção de conhecimento a partir de diversas fontes é essencial. As forças armadas devem estar sempre vigilantes, monitorando as atividades no ciberespaço e identificando potenciais ameaças. A inteligência cibernética, que envolve a coleta e análise de informações sobre possíveis adversários, é uma ferramenta crucial para a segurança nacional. As operações de segurança cibernética, por sua vez, visam proteger as infraestruturas e redes militares, garantindo que estas estejam sempre preparadas para resistir a ataques.

1.3 OPERATION SECURITY (OPSEC) E ANONIMIZAÇÃO

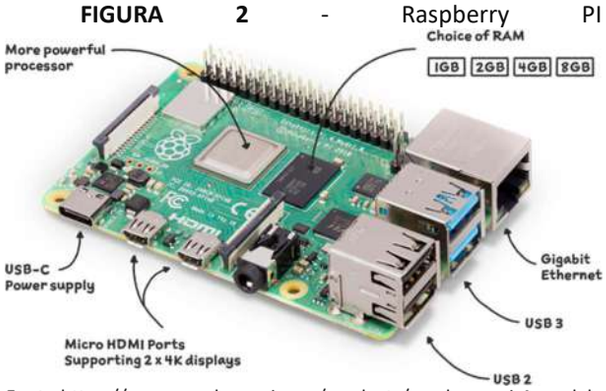
No contexto militar, a segurança da informação e a anonimização são

componentes críticos para o sucesso das operações. O conceito de Operation Security (OPSEC) é fundamental para garantir que informações sensíveis não caiam nas mãos erradas, protegendo as operações e os militares envolvidos. OPSEC envolve uma série de medidas e práticas destinadas a identificar e mitigar riscos de segurança, garantindo que informações vitais sejam mantidas seguras e fora do alcance de adversários.

A anonimização é uma parte crucial do OPSEC, especialmente em operações cibernéticas. No ciberespaço, onde a coleta de informações é uma prática comum, manter a privacidade e a segurança é um desafio constante. As operações militares que envolvem coleta de informações, compartilhamento de dados e comunicação precisam garantir que essas atividades sejam realizadas de forma anônima, para evitar rastreamento e identificação.

Projetos como o gateway de anonimização utilizando o Raspberry Pi, desenvolvido pelo 2º Sargento Lucas da Silva Lemes, exemplificam a importância de soluções tecnológicas acessíveis e eficazes para as forças armadas. Este projeto, que utiliza a rede TOR para permitir a navegação anônima, foi implementado pelo 1º Batalhão de Operações Psicológicas do Comando de Operações Especiais, mostrando-se uma ferramenta valiosa em operações de inteligência e operações especiais.

FIGURA 2 - Raspberry PI



Fonte:https://www.raspberrypi.com/products/raspberry-pi-4-model-b/

Diante da necessidade de aprimorar e expandir essa solução, foram identificadas várias áreas para melhorias. Entre as principais, destaca-se a correção da instabilidade da data e hora do equipamento, que causava problemas na configuração e operação do gateway. Para resolver essa questão, foi implementado um módulo Real Time Clock (RTC), que garante que o dispositivo mantenha a hora correta, independentemente de sua conexão com a internet.

FIGURA 3 - Módulo RTC

Fonte:https://www.makerhero.com/produto/real-time-clock-rtc-ds3231/

Outra melhoria significativa foi a implementação da VPN over TOR, que adiciona uma camada extra de anonimização, garantindo que as comunicações sejam seguras e privadas. No entanto, desafios como a consulta a servidores DNS antes de passar pela rede TOR ainda precisam ser superados para que essa solução seja completamente eficaz.

Este projeto representa um passo importante na direção de fortalecer a segurança cibernética das forças armadas. Embora ainda existam desafios a serem superados, as melhorias implementadas até agora demonstram o potencial dessa solução para operações de inteligência e especiais. A continuidade desse trabalho é crucial para garantir que as forças armadas brasileiras estejam sempre preparadas para enfrentar as ameaças do ciberespaço, protegendo a soberania e a segurança nacional.

CONCLUSÃO

O avanço tecnológico e a crescente interconectividade trouxeram inúmeros benefícios para a sociedade, mas também apresentaram desafios complexos, especialmente no que diz respeito à privacidade e à segurança. No cenário militar, onde a proteção da informação e a anonimização são vitais, a adaptação às novas ameaças cibernéticas tornou-se uma prioridade. As guerras cibernéticas, que transcendem fronteiras físicas, exigem que as forças armadas desenvolvam estratégias sofisticadas para proteger suas operações e garantir a segurança nacional.

O conceito de Operation Security (OPSEC) e as práticas de anonimização destacam-se como elementos cruciais nessa nova fronteira de defesa. A implementação de projetos como o gateway de anonimização utilizando o Raspberry Pi demonstra a importância de soluções tecnológicas inovadoras e acessíveis para manter a segurança cibernética. As melhorias realizadas, como a correção da instabilidade da data e hora e a introdução de VPN over TOR, são passos significativos para o fortalecimento dessas operações.

No entanto, o trabalho está longe de ser concluído. A complexidade das ameaças cibernéticas requer uma abordagem contínua e evolutiva. A busca por soluções para desafios remanescentes, como a gestão de consultas DNS dentro de uma arquitetura de anonimização, é fundamental para consolidar a eficácia das ferramentas desenvolvidas. Portanto, é imperativo que este projeto e outros semelhantes continuem a ser aprimorados e adaptados às necessidades emergentes.

A continuidade das pesquisas e o desenvolvimento de novas tecnologias são essenciais para garantir que as forças armadas brasileiras possam operar com segurança e eficiência no ciberespaço. Somente através de uma abordagem proativa e inovadora será possível proteger a soberania nacional e garantir que o Brasil esteja preparado para enfrentar as ameaças do mundo digital.

REFERÊNCIAS

RASPBERRY PI 4. **Completely upgraded, re-engineered**. Disponível em: https://www.raspberrypi.com/products/raspberry-pi-4-model-b/. Acesso em: 30 agosto de 2024.

EXÉRCITO BRASILEIRO. **Manual de Campanha – Guerra Cibernética**. Brasília, 8 de junho de 2017.

BRASIL. MINISTÉRIO DA DEFESA. **Política Cibernética de Defesa**. Brasília, 21 de dezembro de 2012.

BROWSE PRIVATELY – **Explore Freely** Página inicial. Disponível em: https://www.torproject.org/. Acesso em: 05 julho 2024.

DEBIAN. **Documentação**. Disponível em: https://www.debian.org/doc/index.pt.html. Acesso em: 07 agosto 2024.

IP GEOLOCATION API. **Fast, accurate, reliable**. Disponível em: https://ip-api.com. Acesso em: 06 agosto 2024.

ROMERO, Mario Lobo. **Implementação de um dispositivo portátil de roteamento para redes anônimas baseado em Raspeberry Pi**. (Monografia de Especialização em Redes de Computadores e Teleinformática) – Universidade Tecnológica Federal do Paraná – UTFPR. Curitiba, PR, 2018. Disponível em: https://repositorio.utfpr.edu.br/jspui/handle/1/19974. Acesso em: 31 agosto. 2024.

TAILS. **Conectando à rede Tor**. Disponível em: https://tails.boum.org/doc/anonymous_internet/tor/index.pt.html. Acesso em: 28 agosto. 2024.

MAKER HERO. **Real Time Clock RTC DS3231**. Disponível em: https://www.makerhero.com/produto/real-time-clock-rtc-ds3231/. Acesso em: 31 agosto. 2024.

VIEIRA, Vinícius. **OPSEC. Inteligência Cibernética na prática**, 1ed, 2022.
The Tor Project. Disponível em: https://gitlab.torproject.org/legacy/trac/-/wikis/doc/TransparentProxy#local-redirection-and-anonymizing-middlebox. Acesso em: 31 agosto 2024

A TELEGRAFIA COMO ALTERNATIVA DE COMANDO E CONTROLE NO CENÁRIO DOS CONFLITOS MODERNOS

Sgt Mário Antônio **Costa Souza**
Sgt Jean Carlos **Aguiar da Costa**

Este estudo explora o papel contínuo da telegrafia no cenário militar moderno, com foco na sua aplicação em sistemas de Comando e Controle (C2). Através de uma análise histórica, destaca-se a importância da telegrafia desde o século XIX até os dias atuais, evidenciando sua eficiência em comunicações de longa distância utilizando ondas de alta frequência (HF). O artigo examina a resiliência do código Morse, em situações de conflito, especialmente onde tecnologias modernas podem falhar, como exemplificado na guerra Rússia-Ucrânia. O Exército Brasileiro também é citado, demonstrando a relevância da telegrafia em operações militares contemporâneas, garantindo a continuidade do fluxo de informações em condições adversas. Apesar do avanço das tecnologias de comunicação, a simplicidade e a eficácia da telegrafia continuam essenciais, reforçando a ideia de que soluções básicas podem prevalecer quando sistemas complexos falham.

1. INTRODUÇÃO

A telegrafia, desenvolvida por Samuel Morse e Alfred Vail no século XIX, revolucionou a comunicação a longas distâncias e tornou-se uma ferramenta essencial no meio militar. Usando o código Morse e ondas de alta frequência (HF), a telegrafia oferece um meio de comunicação simples e eficiente.

Em conflitos modernos, como a guerra Rússia-Ucrânia, ela se mostra uma alternativa resiliente diante da vulnerabilidade das tecnologias avançadas. Sua robustez e resistência à interferência a tornam uma opção eficaz para manter o fluxo de informações e a consciência situacional. O Exército Brasileiro, por exemplo, utiliza uma rede de telegrafia em HF que cobre todo o território nacional, a Rede Rádio Fixa (RRF), assegurando comunicações confiáveis em cenários variados de conflitos. Este artigo explora a relevância da telegrafia como alternativa de comunicação para comando e controle em conflitos contemporâneos.

2. DESENVOLVIMENTO

2.1 A Telegrafia e a Revolução da Comunicação Militar

O telégrafo elétrico, criado por Samuel Morse no século XIX, revolucionou as comunicações ao

permitir a transmissão de mensagens a longas distâncias. Nesse sistema, sinais elétricos representavam caracteres do código Morse, compostos por pulsos curtos e longos, transmitidos através de fios de cobre. Letras, números e sinais de pontuação foram codificados em sequências de pontos e traços, formando um padrão internacional de comunicação reconhecido globalmente.

Inicialmente, o telégrafo foi empregado para transmitir mensagens em longas distâncias. Com o tempo, passou a ser utilizado também em rádios e outros transmissores, permitindo o envio rápido de alertas e mensagens cifradas, especialmente útil em navegação marítima e conflitos armados. A eficiência da comunicação por telegrafia melhorou significativamente com a introdução da tecnologia de ondas de alta frequência (HF). As comunicações por HF operam na faixa de 3 MHz a 30 MHz, propagando-se pela ionosfera e possibilitando comunicação a distâncias superiores a 160 km, inclusive além da linha de visada direta, alcançando níveis globais.

A telegrafia, ao utilizar a técnica de ativação e interrupção da portadora com impulsos longos e curtos, permite uma comunicação eficiente, requerendo uma largura de faixa mínima, entre 100 Hz e 200 Hz, e baixa potência para sensibilizar rádios receptores a longas distâncias. A capacidade da telegrafia de ocupar pouca largura de banda, especialmente quando usada em HF, é essencial, visto que nessa faixa de frequência o espectro disponível é limitado, variando de 3 kHz a 20 kHz. Comparada com a fonia (SSB), que tipicamente requer cerca de 2,4 kHz de largura de faixa, a telegrafia demonstra maior eficácia em ambientes com espectro limitado, interferência ou ruído.

2.2 A Telegrafia no Exército Brasileiro

A telegrafia sempre desempenhou um papel fundamental nas comunicações militares, e no Brasil não foi diferente. Desde o século XIX, o Exército Brasileiro reconhece sua importância, adotando-a como um elemento estratégico nas operações militares. Em 11 de maio de 1852, ocorreu a primeira ligação telegráfica no Brasil, conectando o Paço Imperial à Quinta da Boa Vista (RJ) e o Quartel General do Exército ao Campo de Santana (RJ). Essa comunicação, operada pelo Professor Guilherme Schuch Capanema e pelo Coronel Polidoro Quintanilha da Fonseca Jordão, marcou o início de uma nova era nas comunicações militares do país.

A eficácia do telégrafo elétrico em combate ficou evidente durante a Guerra da Crimeia (1854-1856) e influenciou sua adoção pelo Exército Brasileiro durante a Guerra do Paraguai (1864-1870). Sob o comando do Marquês de Caxias, um sistema telegráfico foi instituído, facilitando a coordenação das forças aliadas em manobras decisivas. A telegrafia tornou-se vital durante as duas Guerras Mundiais, com serviços de inteligência focados em decifrar mensagens codificadas em Morse.

Mesmo com os avanços tecnológicos, a telegrafia manteve sua relevância ao longo do século XX. Durante a Revolução de 1964, as comunicações telegráficas foram essenciais para o sucesso das operações militares em um país de vastas dimensões e com desafios de comunicação. Nas operações militares na Amazônia, a telegrafia continua a ser uma ferramenta vital, superando condições adversas que comprometem outros meios de comunicação.

A Escola de Comunicações do Exército Brasileiro desempenha um papel central na preservação e no ensino da telegrafia. A instituição forma especialistas que garantem a eficácia dessa técnica nas operações modernas. Dentro desse contexto, destaca-se a Rede Rádio Fixa (RRF), criada em 1915, como um dos maiores legados operacionais do Serviço Rádiotelegráfico do Exército. A RRF, composta por 12 Centros de Telemática e 156 Estações Rádio distribuídas em todas as guarnições do Exército Brasileiro, transmite mensagens em telegrafia manual (CW), fonia (HF) e dados (TDEx-HF), configurando a maior Rede Rádio HF da América Latina.

A RRF é um pilar das Comunicações do Exército, garantindo comunicações seguras e confiáveis em todo o território nacional, inclusive nas guarnições mais isoladas. Além do código Morse, as estações da RRF utilizam o sistema Tráfego de Dados do Exército em HF (TDEx-HF), que permite a transmissão de dados por meio do equipamento rádio Falcon III 7800H da HARRIS.

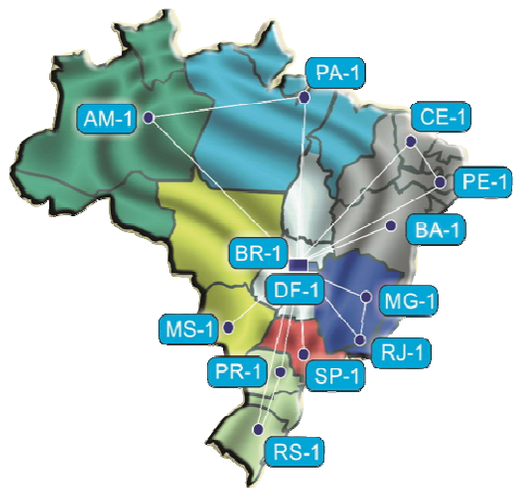


Fig.1: Rede Rádio Fixa Principal.

A integração de tecnologias antigas e modernas reafirma a

importância da RRF como um componente vital do Sistema Estratégico de Comando e Controle do Exército (SEC²Ex), assegurando um fluxo de informações permanente, contínuo e seguro.

2.3 A Telegrafia e o Comando e Controle

2.3.1 O Comando e Controle no Exército Brasileiro

A atividade de Comando e Controle (C²) é essencial para o sucesso das operações militares, pois envolve a ciência e a arte de gerir uma cadeia de comando. Conforme o Manual de Campanha Comando e Controle (EB70-MC-10.205, 1ª Edição, 2023), "O C² constitui-se no exercício da autoridade e da direção que um comandante tem sobre as forças sob seu comando, para o cumprimento da missão atribuída." A tomada de decisões acertadas é fundamental para potencializar a sinergia das forças, especialmente em operações de amplo espectro e em diferentes áreas geográficas.

O mesmo manual destaca a importância da tomada de decisão:

> "A capacidade de os comandantes, em todos os níveis, tomarem decisões acertadas é fundamental para potencializar a sinergia das forças, sob sua responsabilidade, cada vez mais exigidas a atuarem em operações de amplo espectro, as quais podem ser desenvolvidas em áreas geográficas lineares ou não, de forma contígua ou não, buscando contemplar as diversas missões que envolvem o emprego de meios militares."

Portanto, a atividade de C² é crucial para que os comandantes obtenham as informações necessárias para decisões eficazes em um curto espaço de tempo. No contexto dos conflitos modernos, a crescente complexidade das crises e a necessidade de vantagens decisivas tornam o processo decisório cada vez mais dependente de sistemas de Tecnologia da Informação e Comunicações (TIC). O manual de campanha reforça essa dependência:

> "A crescente complexidade das crises e dos conflitos modernos e a necessidade de obtenção de vantagens decisivas nas operações militares tornaram o processo decisório cada vez mais dependente de sistemas de tecnologia da informação e comunicações (TIC) que garantam aos comandantes a execução dos ciclos de comando e controle, com rapidez, precisão e oportunidade."

As informações são, portanto, um ativo estratégico na atividade de C², sendo essenciais para a produção e disseminação do conhecimento em diversos formatos. O fluxo de informações em uma infraestrutura de C² pode ser classificado em dois tipos principais: vertical e horizontal. O fluxo vertical transmite conhecimento do nível tático ao nível político, enquanto o fluxo

horizontal dissemina informações entre elementos do mesmo nível.

Fig.2 – Fluxos de informação de C²

2.3.2 O Emprego Estratégico da Telegrafia como Alternativa de Comando e Controle

A telegrafia, por meio da Rede Rádio Fixa (RRF), é um componente essencial do Sistema Estratégico de Comando e Controle do Exército Brasileiro (SEC²Ex). A RRF assegura comunicações seguras e confiáveis em todo o território nacional, sendo crucial para o planejamento, a direção e o controle das operações militares.

Integrada ao Sistema de Telemática do Exército (SisTEx), a RRF oferece suporte estratégico de comunicações, mesmo em situações de crise, e permite interoperabilidade com outros sistemas de comando e controle.

A operação contínua e a capacidade de transmissão de dados tornam a RRF um pilar na infraestrutura de comunicações do Exército, garantindo a eficiência e a resiliência do SEC²Ex. A telegrafia se destaca por sua robustez e pela capacidade de operar em canais de alta frequência (HF) com largura de banda limitada, permitindo comunicações a grandes distâncias, mesmo em condições de espectro restrito.

Utilizando-se de ondas contínuas em formato analógico/manual, a telegrafia já demonstrou seu valor ao operar com largura de faixa mínima em HF para envio e recebimento de informações via código Morse. Sua capacidade de codificar mensagens de forma rápida e eficaz é crucial para as comunicações militares durante os conflitos. Além disso, a utilização das ondas de HF com modulação digital possibilita uma transmissão eficiente de dados, mesmo com uma relação sinal-ruído desfavorável.

Nesse contexto, a telegrafia via ondas de HF configura-se como uma infraestrutura alternativa viável para a manutenção do fluxo de informações nos processos de tomada de decisão, fundamentais para o Comando e Controle. Sua utilização contribui significativamente para a obtenção da consciência situacional em ambientes operacionais complexos.

2.3.3 Integração com Outras Tecnologias

Durante a Segunda Guerra Mundial, o avanço das comunicações de alta frequência (HF) sem fio, como os rádios de ondas curtas, trouxe maior flexibilidade para as operações militares. As técnicas de modulação de frequência (FM) tornaram-se mais prevalentes devido à sua superior relação sinal-ruído e maior resistência à interferência. Essa modulação aprimorou significativamente a qualidade da comunicação em ambientes de combate, onde interferência e ruído eram frequentes.

Apesar do surgimento de novas tecnologias, a integração da tecnologia HF com o código Morse manteve-se um padrão, graças à sua confiabilidade e eficácia. A telegrafia em HF continuou a ser uma solução eficiente para transmitir informações, mesmo em condições adversas, consolidando-se como uma ferramenta vital para a comunicação militar.

3. Emprego da Telegrafia no Atual Cenário Militar

No conflito entre Rússia e Ucrânia, onde tecnologias modernas como drones e mísseis hipersônicos predominam, porém o código Morse continua a desempenhar um papel crucial nas comunicações militares. Embora simples, esse sistema de codificação tem se mostrado eficaz e resiliente, oferecendo vantagens valiosas em cenários de combate contemporâneos. O código Morse é especialmente útil em situações onde a infraestrutura de comunicação é alvo de ataques e sabotagens. Em ambientes de combate como na Ucrânia, as linhas de comunicação são frequentemente atacadas, e tecnologias modernas podem falhar devido a interferências, ataques cibernéticos ou danos físicos. A simplicidade e a robustez do Morse o tornam uma alternativa confiável quando outros métodos se tornam inviáveis, possibilitando operações com equipamentos simples mesmo em condições adversas.

Uma das principais vantagens do código Morse é seu baixo consumo de energia. Em situações onde os recursos são escassos, a capacidade de transmitir mensagens com apenas 78 miliwatts de potência é significativa, permitindo comunicação constante mesmo sob restrições energéticas. Essa eficiência energética é vital para manter o comando e controle das tropas em campo.

A robustez do Morse em ambientes de alta interferência também é uma vantagem importante. Ele utiliza uma largura de banda estreita (100-150 Hz), tornando-se menos suscetível a

interferências em comparação com outros métodos de comunicação. Em conflitos como o da Ucrânia, onde sinais são frequentemente perturbados, o Morse se destaca por transmitir mensagens claras e legíveis, garantindo uma comunicação eficaz.

Fig. 3 – Militar russo em operação
Foto Reprodução/Anatolii STEPANOV / AFP)

O uso contínuo do código Morse pelas forças russas e outras frações no conflito demonstra sua capacidade de fornecer uma comunicação segura e discreta. Mesmo em um cenário militar moderno, sua simplicidade e confiabilidade mantêm-no como uma ferramenta essencial, especialmente em situações de emergência onde outras formas de comunicação falham. A persistência do Morse destaca sua durabilidade e relevância ao longo dos anos.

4. Conclusão

O código Morse, uma invenção do século XIX, continua a desempenhar um papel crucial nas comunicações militares modernas, como evidenciado pelo conflito entre Rússia e Ucrânia.

Embora possa parecer ultrapassado em comparação com os sistemas de comunicação avançados atuais, sua simplicidade, eficiência energética e robustez em condições adversas o tornam uma ferramenta indispensável para comando e controle em cenários de guerra contemporâneos.

A capacidade de operar com equipamentos simples, mesmo em condições extremas e com recursos limitados, demonstra sua resiliência. Em ambientes de combate onde a infraestrutura de comunicação é alvo de ataques e as tecnologias modernas podem falhar devido a interferências e ataques cibernéticos, o código Morse se apresenta como uma alternativa confiável e segura. Seu baixo consumo de energia e operação em largura de banda estreita são particularmente úteis em contextos onde o gerenciamento de recursos e a minimização de interferências são críticos.

A persistência do código Morse no cenário militar atual reflete sua importância histórica e a confiança em suas capacidades. A integração do Morse com tecnologias modernas, como sistemas de alta frequência (HF), assegura uma infraestrutura de

comunicação robusta e eficaz, mantendo o fluxo de informações essencial para comando e controle, mesmo em condições desafiadoras.

Em linhas gerais, a análise do uso do código Morse em conflitos contemporâneos, como o da Rússia-Ucrânia, destaca sua relevância contínua. Sua adaptabilidade e eficácia em ambientes de alta interferência e recursos limitados mostram que, mesmo com a evolução tecnológica, a simplicidade e robustez do código Morse permanecem valiosas.

Em síntese, ele não apenas complementa, mas também reforça a infraestrutura de comunicação militar, reafirmando-se como uma ferramenta vital para a segurança e eficácia das operações em cenários de conflito moderno. Quando o complexo falha, o simples prevalece.

ABSTRACT

This study explores the continuing role of telegraphy in the modern military scenario, focusing on its application in Command and Control (C2) systems. Through a historical analysis, the importance of telegraphy from the 19th century to the present day is highlighted, evidencing its efficiency in long-distance communications using high frequency (HF) waves. The article examines the resilience of Morse code in conflict situations, especially where modern technologies can fail, as exemplified in the Russia-Ukraine war. The Brazilian Army is also cited, demonstrating the relevance of telegraphy in contemporary military operations, ensuring the continuity of the flow of information under adverse conditions. Despite the advancement of communication technologies, the simplicity and effectiveness of telegraphy remain essential, reinforcing the idea that basic solutions can prevail when complex systems fail.

5. REFERÊNCIAS:

BRASIL. Exército. Comando de Operações Terrestre. Manual de Campanha Comando e Controle - EB70-MC-10.205. Brasília: EB, 2023.

BRASIL. Exército. Estado-Maior do Exército. Diretriz Organizadora do Sistema Estratégico de Comando e Controle do Exército (EB20-D-02.037), 1ª ed. Brasília: EME, 2024.

BRASIL. Exército. Estado-Maior do Exército. Manual de Campanha C 24-18 – Emprego do Rádio em Campanha, 4ª ed. Brasília: EME, 1997.

BRASIL. Exército Brasileiro. Estado-Maior do Exército. Exploração em Radiotelegrafia e Telegrafia. EB70-MT-10.409. 1ª ed. Brasília: COTER, 2022.

DEMENICIS, L. S. A Rede Rádio HF como Mitigação dos Efeitos das Ameaças Cibernéticas nas Redes de Comunicação Estratégica do Exército Brasileiro. 2023. Trabalho de Conclusão de Curso (Curso Superior de Segurança

e Defesa Cibernética) – Escola Superior de Guerra, Rio de Janeiro, 2023.

GUITARRARA, Paloma. Código Morse. Brasil Escola. Disponível em: https://brasilescola.uol.com.br/geografia/codigo-morse.htm. Acesso em: 25 ago. 2024.

INGESSON, Tony. Ukraine war: why the Russian army is still using Morse code. 2024.

LARANJEIRA, Francisco. Ucrânia: na guerra moderna ainda há uma tecnologia com mais de 150 anos a dar cartas. Ou 'bipes'... Executive Digest, 2024. Disponível em: https://executivedigest.sapo.pt/noticias/ucrania-na-guerra-moderna-ainda-ha-uma-tecnologia-com-mais-de-150-anos-a-dar-cartas-ou-bipes/. Acesso em: [colocar data de acesso, se aplicável].

POR QUE, numa guerra moderna, com mísseis e drones, a Rússia ainda usa código Morse? BBC News Brasil, 21 maio 2024. Disponível em: https://www.bbc.com/portuguese/articles/clmmlk547rjo. Acesso em: 25 ago. 2024.

GUERRA NA UCRÂNIA: O AUDIOVISUAL COMO ARMA NA CONQUISTA DA GUERRA DE NARRATIVAS DO COMBATE MODERNO

Sgt THIAGO **CARBOS** DA SILVA
S Ten **GLAUBER** VIANA FERNANDES

RESUMO

Na guerra moderna, o campo de batalha não se limita apenas ao uso de armas e estratégias militares; as narrativas também desempenham um papel crucial. Na Guerra na Ucrânia, o audiovisual tornou-se uma poderosa ferramenta na construção e disseminação dessas narrativas. Tanto fotógrafos quanto cinegrafistas ucranianos e russos estão na linha de frente dessa guerra de narrativas, capturando imagens que não só documentam a realidade do conflito, mas também moldam a percepção global sobre os eventos. Este artigo explora o impacto dessas imagens no imaginário público, analisa como cada lado utiliza o audiovisual para seus objetivos estratégicos e discute a importância do controle da narrativa na conquista da opinião pública.

Palavras-chave: guerra na Ucrânia, guerra de narrativas, opinião pública, audiovisual em combate.

1 INTRODUÇÃO

A Guerra na Ucrânia trouxe à tona o poder do audiovisual na guerra de narrativas. Desde o início do conflito, as imagens capturadas por fotógrafos e cinegrafistas se tornaram armas poderosas, capazes de influenciar a opinião pública e moldar a percepção do mundo sobre a guerra. Tanto ucranianos quanto russos utilizam esses recursos para seus próprios fins, tentando vencer não apenas no campo de batalha físico, mas também no psicológico de cada indivíduo. A guerra moderna é travada em múltiplas frentes, e o controle da narrativa é uma das mais importantes. Neste contexto, as imagens capturadas no campo de batalha são essenciais, pois têm o poder de transcender fronteiras, provocar emoções e até mesmo moldar decisões políticas. Este artigo pretende examinar como o audiovisual tem sido utilizado como arma na Guerra na Ucrânia, destacando o trabalho dos fotógrafos e cinegrafistas de ambos os lados.

2 DESENVOLVIMENTO

2.1 A EVOLUÇÃO DO AUDIOVISUAL COMO FERRAMENTA DE GUERRA

Historicamente, a fotografia e o cinema têm desempenhado papéis importantes em conflitos armados, desde a Guerra Civil Americana até as guerras mundiais. No entanto, a Guerra na Ucrânia representa um novo capítulo nessa história, onde o avanço tecnológico e a onipresença das redes sociais amplificam o poder do audiovisual. Hoje, qualquer pessoa com um smartphone pode capturar imagens e vídeos que rapidamente se espalham pelo mundo, moldando a narrativa de uma guerra antes mesmo que os fatos sejam verificados.

Na Guerra na Ucrânia, esse fenômeno é evidente. Tanto os ucranianos quanto os russos entendem o poder da imagem e a utilizam de maneira estratégica. A Ucrânia, por exemplo, tem utilizado o audiovisual para destacar a resistência e a resiliência de seu povo, frequentemente mostrando civis em situações de grande dificuldade e soldados em atos de bravura. Essas imagens são projetadas para gerar empatia e apoio internacional, fortalecendo a narrativa de uma nação que luta por sua sobrevivência contra uma invasão externa. Como exemplo, temos a fotografia (figura 1) e o vídeo do soldado Tymofiy Shadura, que em um ato heróico, antes de ser fuzilado por russos, disse o brado histórico ucraniano “Slava Ukraini” (glória àUcrânia) e por essa atitude uma estátua foi construída em sua homenagem (figura 2).

(figura 1)

(figura 2)

Por outro lado, a Rússia também utiliza o audiovisual, mas com uma abordagem diferente. A propaganda russa muitas vezes se concentra em deslegitimar a resistência ucraniana, pintando-a como uma ameaça controlada por forças ocidentais. Imagens que mostram destruição, mas com uma narrativa que sugere que os ucranianos são os responsáveis por suas próprias tragédias, têm sido comuns. Além disso, a Rússia tenta controlar a narrativa dentro de suas próprias fronteiras, restringindo o acesso à mídia ocidental e promovendo uma visão unificada do conflito que apoia as ações do governo.

2.2 O PAPEL DOS FOTÓGRAFOS E CINEGRAFISTAS NO CAMPO DE BATALHA

Fotógrafos e cinegrafistas desempenham um papel fundamental na construção dessas narrativas. Eles arriscam suas vidas para capturar imagens que podem mudar o curso de uma guerra. No lado ucraniano, muitos fotógrafos se tornaram símbolos de resistência, suas imagens servindo como lembretes constantes do custo humano da guerra, como a fotografia do brasileiro Felipe Dana, ganhador do prêmio Pulitzer de fotografia, como a melhor fotografia de guerra em 2023, fotografia que mostra um cachorro junto ao corpo da sua dona morta após um bombardeio russo na cidade de Bucha (figura 3). Alguns têm documentado a vida nas trincheiras, a devastação em cidades bombardeadas e os rostos dos sobreviventes, criando um arquivo visual que é tanto um testemunho da guerra quanto uma ferramenta de mobilização.

(figura 3)

No lado russo, o trabalho dos fotógrafos e cinegrafistas é mais controlado, mas não menos impactante. O governo russo mantém um controle rígido sobre o que pode ser mostrado e como deve ser interpretado. Mesmo assim, alguns profissionais têm conseguido capturar a realidade do conflito de uma maneira que desafia as narrativas oficiais. Esses registros são frequentemente disseminados por meios alternativos, desafiando a narrativa unificada do Kremlin e oferecendo ao mundo um vislumbre do lado menos glamoroso da guerra.

Nessa guerra, destaca-se em especial duas dimensões em que o conflito é travado: uma relacionada à natureza informacional e de propaganda, e outra relativa à guerra econômica, por meio das sanções impostas à Rússia, em especial pelos países do G7. No primeiro caso, destaca-se a "guerra de narrativas", um velho lugar comum no que diz respeito à guerra – a ideia de que, na guerra, a primeira vítima é a informação –torna-se ainda mais verdadeiro com a instantaneidade da informação possibilitada pelo advento das redes sociais em escala planetária. Aliás, o uso de celular na frente de batalha, em especial da plataforma TikTok pelos soldados ucranianos, tem sido uma das vedetes da atual guerra. Ressalte-se ainda, na dita "guerra de narrativas", a extraordinária mobilização dos grandes conglomerados de comunicação norte-americanos e europeus, de forma quase uníssona, em torno da narrativa ucraniana da guerra e também da midiática figura de seu presidente, Vladimir Zelensky, ele próprio, aliás, tendo ascendido na política após exitosa carreira na TV local. Diante da demonização da figura do líder russo, para além de qualquer juízo de valor sobre sua figura, é fato que, na guerra informacional, a vitória ucraniana ancorada nesses fatores é inconteste. (CARMONA, 2024).

2.3 O IMPACTO DAS IMAGENS NA OPINIÃO PÚBLICA

A força de uma imagem reside em sua capacidade de evocar emoções imediatas. Imagens de cidades destruídas, soldados em ação ou civis feridos, como a imagem do hospital infantil oncológico atingido por um bombardeio russo em Kiev (figura 4), não só informam, mas também moldam percepções. Em muitos casos, essas imagens podem influenciar diretamente a opinião pública e, por extensão, as políticas governamentais. Na Guerra na Ucrânia, as imagens capturadas pelos fotógrafos e cinegrafistas têm sido fundamentais para manter a atenção do mundo voltada para o conflito, evitando que ele seja esquecido em meio a outros eventos globais.

(figura 4)

No entanto, o poder das imagens também traz desafios. A manipulação de fotos e vídeos, a falta de contexto e a propaganda descarada podem distorcer a realidade e enganar o público. Em um conflito onde a verdade é muitas vezes a primeira vítima, a responsabilidade dos fotógrafos e cinegrafistas em capturar e disseminar imagens verídicas é mais importante do que nunca.

3. CONCLUSÃO

A Guerra na Ucrânia demonstrou que, no combate moderno, o controle da narrativa é tão vital quanto o controle do território. As imagens capturadas por fotógrafos e cinegrafistas desempenham um papel crucial na formação dessas narrativas, influenciando a opinião pública e, em última análise, as decisões políticas.

Tanto ucranianos quanto russos utilizam o audiovisual como uma arma poderosa na guerra de narrativas, cada lado tentando moldar a percepção do conflito de acordo com seus próprios interesses. Em um mundo onde a informação é instantânea e global, a luta pelo controle das imagens e das histórias que elas contam tornou-se uma das frentes mais importantes da guerra moderna.

Abstract

In modern warfare, the battlefield is not just limited to the use of weapons and military strategies; narratives also play a crucial role. During the War in Ukraine, audiovisual media became a powerful tool in the construction and dissemination of these narratives. Both Ukrainian and Russian photographers and videographers are on the front lines of this war of narratives, capturing images that not only document the reality of the conflict, but also shape global perceptions of the events. This article explores the impact of these images on the public imagination, analyzes how each side uses audiovisual for its strategic objectives and discusses the importance of controlling the narrative in winning public opinion.

Keywords: (war in Ukraine, war photography, war narratives, public opinion, audiovisual in combat.)

4. REFERÊNCIA

CARMONA, Ronaldo. A guerra na Ucrânia: uma análise geopolítica. Cebri, 2024. Disponível em: https://cebri.org/revista/br/artigo/46/a-guerra-na-ucrania-uma-analise-geopolitica. Acesso em: 30 de

BRASIL, NOVEMBRO DE 1935: ANÁLISE DO COMANDO E CONTROLE DAS FORÇAS INVASORAS

Sgt **J***UAN MARTINEZ* **BENDER**
S*gt* **VICTOR** *DE CARVALHO* **MATTOS** *CAVALCANTE*

RESUMO

No período entre guerras, quando Forças Armadas de todo o mundo ainda processavam o avanço das Comunicações HF evidenciado na Primeira Guerra, uma infiltração estrangeira foi empreendida sem sucesso em solo brasileiro. O presente artigo tem por objetivo analisar a estrutura e o planejamento de comunicações, empregados pelas forças invasoras, no evento que se tornaria marco na história militar e do país: a Intentona de novembro de 1935. Por meio de uma revisão bibliográfica, constatou-se que, a despeito do financiamento soviético, as falhas de Comando e Controle contrastam com a ambição do empreendimento e concorreram para o seu fracasso.

Palavras-chave: História Militar. Comando e Controle. Intentona de 1935.

1 INTRODUÇÃO

Quando a URSS se desintegrou em 1991, a abertura dos primeiros arquivos de Moscou possibilitou a confirmação de detalhes sobre a investida soviética, ocorrida em 1935, em solo brasileiro. O pioneiro estudo dessa documentação, empreendido pelo jornalista William Waack, resultou na elaboração do livro *Camaradas: nos arquivos de Moscou*. É no esforço de estabelecer um diálogo entre as informações contidas na referida obra e os princípios de Comando e Controle, extraídos do Manual EB20-MC-10.205, que o presente artigo visa discorrer sobre os dados disponíveis acerca das Comunicações empregadas em um episódio decisivo de nossa História Militar.

Como forma de complemento ao estudo, foram consultadas fontes bibliográficas que circundam o tema, tais como o trabalho historiográfico do general José Campos de Aragão acerca dos inquéritos e boletins da Intentona; e a tese de doutorado do historiador Rodrigo Patto de Sá Motta, que versa sobre o estudo do anticomunismo no Brasil.

2 O RÁDIO OPERADOR DE MOSCOU

Na madrugada de dezoito para dezenove de novembro de 1935, as festividades de um evento restrito ecoaram no interior de um apartamento em Copacabana, no Rio de Janeiro. Tratava-se da comemoração pelo serviço, enfim concluído, do rádio operador Victor Allen Baron – um agente de Moscou designado para a montagem do rádio transmissor que conectaria o Brasil à União Soviética, naquela que seria a grande missão da vida de Victor.

O primeiro contato deveria ter ocorrido em 21 de setembro; contudo, para o desespero do comunicante, a recepção perfeita dessa primeira tentativa de transmissão contrastou com o absoluto silêncio-rádio do outro lado da rede, indicando falha no estabelecimento do enlace[i].

De julho a agosto, Baron esteve empenhado na montagem artesanal que aprendera na secreta escola de rádio e comunicações, localizada na então capital do mundo comunista. Considerando a realidade tecnológica da época, parte importante da formação do rádio operador soviético consistia na capacitação para a montagem de seu próprio aparelho transceptor, no posto, quase sempre avançado e isolado, onde a ação deveria ocorrer[ii]. Devido a tuberculose e sífilis de Baron, os demais

integrantes da equipe preocupavam-se quanto a sua baixa imunidade perante os "possíveis percalços" de uma eventual prisão.

Já eram patentes o desgaste físico e a lentidão oriunda, entre outros motivos, pela pressão inerente aos procedimentos básicos de segurança das comunicações tais como a transmissão em código morse e o minucioso uso de grupos cifrados de cinco letras. Para autenticação, seriam utilizadas, ainda, as primeiras três letras de uma página pré-estabelecida, ajustada para a posição vertical do livro *Man with talent.*

Naquela noite de comemorações de dezenove de novembro, porém, as dificuldades pareciam enfim superadas na Estação Rádio de Copacabana. A rede rádio fora finalmente aberta com "saudações revolucionárias" e "abraços bolchevistas". A missão finalmente estava pronta para começar - seria a última do jovem Victor Baron.

3 O ELO DE LIGAÇÃO

Cotado para um alto posto militar no movimento de outubro de 1930, a recusa do líder tenentista, Luís Carlos Prestes, em participar da revo-lução que alçou Getúlio Vargas ao poder, não o impediu de aceitar o dinheiro ofertado em troca de sua participação. "Ele o guardaria para financiar sua própria revolução" nos diz Waack (1993, p.29) - ironicamente, uma revolução empreendida contra o próprio governo Vargas.

O dinheiro entregue a Prestes acabaria por servir como bilhete de ingresso aos círculos do Partido Comunista da União Soviética, o qual, até sua desintegração em 1991, manteria estrito controle da direção política do Partido Comunista Brasileiro (PCB), fundado em 1922. Os arquivos pesquisados por Waack indicam que os fundos proporcionados por Prestes, além de alçá-lo membro do comitê executivo da IC, junto a nomes como Stalin e Mao Tsé-tung[iii], possibilitou o financiamento de diversos partidos comunistas na América do Sul até, pelo menos, o final de 1933. O montante de cerca de 80 mil dólares dedicados à operação brasileira, no entanto, não passava de 5% do que o Exército Vermelho investira com espionagem em países como Alemanha, Grã-Bretanha e Estados Unidos[iv].

Ao longo da década de 1930, enquanto militares ligados ao governo ocupavam cargos estratégicos em áreas como Comissão de Siderurgia e Conselho Nacional do Petróleo, nos bastidores da tropa uma ameaça pairava em silêncio. Beneficiado pelo surto de indisciplina do início dos anos 1930, o PCB colhia os primeiros frutos do fiel cumprimento da diretriz soviética emitida no II Congresso da Internacional, em Moscou, segundo a qual: a expansão da ideologia soviética para os demais países deveria ocorrer por meio da infiltração política em setores estratégicos, entre eles, sindicatos e quartéis[v].

A construção da imagem de líder atribuída à Carlos Prestes, em torno do qual forjou-se a promessa de dias melhores, foi, portanto, fortalecida pelo descontentamento com soldo e redução de efetivos. Finalmente, em 5 de julho de 1935, um manifesto foi emitido conclamando as Forças Armadas a apoiarem a Aliança Nacional Libertadora na realização de uma "revolução imediata". Quem o assinava era Carlos Prestes. Como resposta, amparado na recém criada Lei de Segurança Nacional[vi], o presidente Getúlio Vargas decretou a ilegalidade da ANL, seguindo-se o imediato fechamento de 1,5 mil núcleos estruturados pelo Brasil. Os documentos apreendidos confirmaram a existência de uma tentativa de golpe de Estado em marcha[vii]. Ainda que clandestina, porém, uma ligação entre a ANL e militares vinha sendo estabelecida. De acordo com Moraes e Viana (1982 apud Vicentino, 2009, p.360):

> O próprio Prestes mais tarde diria: "[...] era muito mais fácil construir o partido (comunista) dentro dos quartéis do que

insurreição. Segundo Reis (2014, p.182), Prestes acreditava que uma vitória localizada se irradiaria rapidamente por todo o território brasileiro. Sua consciência situacional, no entanto, era precária e se limitava à área militar - o que o isolava, portanto, dos demais fatores imprescindíveis à tomada de decisão[xx].

Quando a revolta finalmente eclodiu em Recife - a despeito de uma significativa distribuição de armas a populares - a esperada adesão popular em massa, inerente ao êxito da esperada revolução, não aconteceu[xxi].

5 COMANDO E DESCONTROLE

Fator de sucesso ou fracasso nas operações, o Comando e Controle - entendido como o exercício da direção que um comandante tem sobre as forças comandadas, para o cumprimento da missão - é um indicador reconhecidamente decisivo para a competência gerencialxxii. No tocante à Intentona, trancado em um QG improvisado no bairro de Vila Isabel, no Rio, o capitão encarregado pela URSS de comandar a revolução não sabia o que se passava no front. De acordo com Waack (1993, p.232):

> Às cinco da manhã, um mensageiro anunciou que a Vila Militar, onde se concentravam 10 mil soldados do Exército, havia aderido à insurreição. Quinze minutos depois, outro mensageiro chegou dizendo que a Vila Militar estava do lado do governo. Às oito da manhã, com Martins avisando que a Escola de Aviação Militar havia se rebelado (nesse exato momento os revoltosos nessa unidade estavam se rendendo).

Agravando a situação, diante do fluxo de informações desencontradas e contraditórias, Prestes e as lideranças do Comitê Central passaram a utilizar como fonte para a tomada de decisão a repercussão noticiada pela imprensa convencional. Em um comparativo qualitativo das comunicações internas e externas, utilizadas para a operação, constata Reis (2014, p.185):

> Se com Moscou as comunicações tinham alcançado certo nível de sofisticação, através de um fluxo regular de telegramas codificados e até de um rádio transmissor-receptor, montado, afinal, por Victor Baron, em fins de novembro, o sistema de comunicações do Partido dentro do país continuava, como sempre fora, muito precário.

Entre os documentos secretos apreendidos após o fracasso do golpe, encontra-se um radiograma datado de 3 julho de 1935, que especificava quais unidades, naquele momento, teriam supostamente declarado apoio às ordens de Prestes. Entre elas, de acordo com Waack (1993, p. 161), estariam unidades militares localizadas em São Paulo, Santa Catarina, Piauí e Ceará, além dos cinco principais fortes no Rio de Janeiro, uma companhia de metralhadoras e dois regimentos de artilharia pesada. De fato, três unidades militares que aderiram quase inteiramente ao movimento, o 21° BC, o 29° BC e o 3° RI, acabariam posteriormente extintas por decreto presidencial[xxiii]. Ainda sobre o valor qualitativo dos documentos deixados por Prestes:

> Esses papéis não apenas comprovavam as conexões internacionais do movimento, o que em si já se constituía em apreciável reforço propagandístico, que o governo Vargas soube utilizar com eficiência. Os mais de mil documentos apreendidos, segundo os autos policiais, permitiam uma visão em profundidade dos objetivos, métodos e estrutura da organização do Bureau Sul-Americano do Komintern, e não apenas no Brasil (Waack, 1993, p.255).

Se, no plano interno, a liderança autocrática[xxiv] de Prestes levou a falhas de segurança; no plano externo, houve também falha no princípio da rapidez[xxv]. Na manhã de 27 de novembro, um radiograma oriundo de Moscou,

> nas fábricas. Depois do movimento de 30, estabeleceu-se uma grande anarquia nas Forças Armadas. Mas havia uma falha: o trabalho não era feito no sentido de organizar os soldados para apoiar o movimento operário. Era um trabalho meramente agitativo.

Em 1935, mesmo clandestina desde 12 de julho, a ANL contava com ramificações em áreas estratégicas como Polícia Militar, Corpo de Bombeiros e Guarda Civil. Controlada pelo PCB, a organização passara, por consequência, a receber o apoio do Komintern em Moscou[viii]. Naqueles meses de 1935, enquanto Victor Baron preparava seu equipamento rádio, panfletos clandestinos circulavam em quartéis visando a convocação das praças para uma revolução armada.

4 O PLANEJAMENTO E A REDE RÁDIO

Em caráter simbólico, Prestes escolheu o mês de novembro, tão representativo para os simpatizantes da Revolução Russa de 1917. Ainda que a eclosão do movimento estivesse a cargo de militares coaptados, houve, desde o início, a expectativa de adesão de civis que seriam armados após a tomada dos quartéis. Esse plano concretizou-se nas insurreições do Nordeste, mas não se repetiu no Rio de Janeiro dado o grau de preparação com a quebra do elemento surpresa ocasionado pela antecipação em Natal. O motivo desse adiantamento possui diferentes versões: a primeira delas, é associada a um erro de Comunicações. O dia “D” da Intentona seria originalmente o 5 de dezembro, porém, a falha procedimental que acoplou ao invés de somar os co-dinúmeros 2 e 3, acabou precipitando o movimento para 23 de novembro[ix]. A segunda versão atesta que o adiantamento do levante deve-se, na verdade, ao comando do 21º BC, de Natal, que, na segunda-feira, dia 25, resolveu promover a baixa de alguns soldados e cabos ligados ao PCB. Por essa razão, a célula comunista do batalhão teria, por conta própria, optado pela antecipação da Intentona[x].

Quanto ao planejamento da ação, os arquivos de Moscou indicam que a Intentona, a princípio, não deveria parecer um empreendimento soviético, mas sim uma insurreição autônoma e anti-imperialista vinculada aos ideais da coluna Prestes - monitoradas desde 1927 pela URSS[xi].

A ligação, no entanto, ficaria clara logo que desarticulada, graças à insistência do "cavaleiro da esperança[xii]" em negligenciar normas de segurança, como por exemplo a determinação de que todos os documentos deveriam ser queimados[xiii]. A distribuição de postos rádios de transmissão, no enlace entre Moscou e Brasil, possibilitou não apenas o conhecimento das atividades do Komintern na América Latina, mas o vazamento do retorno clandestino de Prestes ao Brasil.

No quesito segurança das comunicações, Prestes cometeu erros de toda sorte, alguns incompatíveis com a experiência militar pela qual era co-nhecido. Mesmo o assessoramento da agente do serviço soviético, Olga Benário, não foi suficiente para que Prestes evitasse de despachar estafetas para contatar militares dos quais o capitão sequer tinha certeza se estariam dispostos a pegar em armas contra o governo[xiv].

Em fins de junho o serviço secreto inglês alertara o governo brasileiro da concentração de forças soviéticas no Brasil[xv]. Na Rede Rádio que ora se instalava, postos de retransmissão radiotelegráfica foram descentralizados em cidades europeias[xvi], tendo Paris recebido o indicativo de N26; e Genebra o indicativo N17. Quanto à Estação montada no Rio de Janeiro, esta ficaria com o indicativo N20[xvii]. Alguns autores discutem a possibilidade de que um dos agentes envolvidos na Intentona, Johann de Graaf, fosse, na verdade, um duplo espião a serviço do serviço de inteligência britânico[xviii].

As informações repassadas por Prestes a fim de subsidiar a tomada de decisão na sede do PCUS[xix], em Moscou, eram otimistas e superestimavam as condições para a eclosão da

recebido pela Estação de Copacabana, autorizava enfim a eclosão do levante armado. Naquele instante, a Intentona Comunista havia começado já havia quatro dias, por meio do 21º Batalhão de Caçadores, em Natal[xxvi]. Quando o radiograma de autorização deu entrada na Estação N20, o movimento já dava seus últimos suspiros[xxvii]. Era o fim da primeira e mais significativa incursão armada e estrangeira, de caráter comunista, em solo brasileiro; aquela que, junto a outras tentativas esparsas - Bulgária e Alemanha em 1923, Indonésia em 1926, China em 1927 - seria descrita pelo historiador Eric Hobsbawm (1995, p.77) como "tardia, desastrosa e anômala".

6 ANÁLISE PÓS AÇÃO

No dia 27, vencido o 3º RI, no Rio de Janeiro, Unidade que, caso vitoriosa, avançaria sobre o Palácio Guanabara, onde residia o presidente (Reis, 2014, p. 187), o jornal *A Manhã* fez circular um atrasado manifesto escrito dias antes por Prestes cujo título anunciava: "Carlos Prestes à frente da insurreição armada no Rioxxviii**"**. Um relatório do Serviço Secreto Soviético (KGBxxix) de 1969, demonstra que dirigentes do PCB responsabilizam Prestes não apenas pelos vazamentos de arquivos secretos da Intentona, mas também por outros dois ocorridos em 1947 e 1964xxx.

O rastro de pistas deixado pelo capitão possibilitou que a polícia o surpreendesse de pijama, na alvorada de 5 de março de 1936. É possível que o informe decisivo tenha sido fornecido por ninguém menos que o rádio operador Victor Baron, antes de suicidar-se, pulando do edifício da Polícia Central do Rio de Janeiro[xxxi].

Na ocasião da prisão de Prestes, uma grávida Olga Benário cumpriu a missão que lhe fora confiada em Moscou: colocou-se diante do comandante derrotado, salvando-lhe a vida[xxxii]. Como a história se encarregaria de mostrar, a jovem agente secreta não teria a mesma sorte[xxxiii].

Uma série de indicadores permitem supor que a Intentona tinha potencial para um alcance maior caso não tivesse sido precipitada em Natal[xxxiv]. Entre os subsídios para tanto constam a panfletagem recolhida[xxxv] e a prisão de militares em quartéis pelo país, flagrados e frustrados na tentativa de provocar novas agitações[xxxvi]. Mais do que isso, Motta observa que a Internacional Comunista deslocou para o Brasil um número de agentes em quantidade superior ao "considerado normal" - cerca de dez, dentre eles, especialistas em bombas e em radiotransmissões[xxxvii].

7 CONCLUSÃO

A partir da bibliografia analisada, é possível concluir que as negligências de Comando e Controle, em especial, no âmbito da administração das informações, foram decisivas para o fracasso da investida soviética de 1935 no Brasil. Ainda que a expressão "Intentona" seja considerada desonrosa por determinados setores simpáticos à açãoxxxviii, a designação é etimologicamente correta, já que "intentona" significa "intento louco, plano insensato", o que, para Boris Fausto (2006, p.75), bem corresponde ao episódio.

A despeito do saldo inconclusivo de mortes[xxxix], o planejamento da Intentona se mostra frágil, beirando ao relapso, diante das pretensões revolucionárias do levante. Quanto aos seus impactos psicossociais, no entanto, cabem ainda estudos. O episódio é uma peça do quebra-cabeças para quem busca compreender o posicionamento das Forças Armadas, uma década à frente, quando a Guerra Fria dividiu o mundo em ideologias antagônicas. Anualmente, desde 1936, uma cerimônia[xl] é realizada, frente ao monumento-túmulo, em Praia Vermelha, onde constam o nome de 31 militares legalistas que tombaram no massacre[xli].

Abstract
In the interwar period, when Armed Forces around the world were still processing the advancement of HF Communications evidenced in the First War, foreign infiltration was undertaken unsuccessfully on Brazilian soil. This article aims to analyze the structure and planning of communications, used by the invading forces, in the event that would become a milestone in the military and country's history: the Intentona of November 1935. Through a bibliographical review, it was found that, despite Soviet financing, Command and Control failures contrasted with the ambition of the enterprise and contributed to its failure.

Keywords: *Military History. Command and Control. Intentone of 1935.*

8 REFERÊNCIAS

AUGUSTO, Agnaldo Del Nero. **A grande mentira**. Rio de Janeiro: Biblioteca do Exército, 2001.

ARAGÃO, Campos de. **A intentona comunista de 1935**. Rio de Janeiro: Biblioteca do Exército, 1973.

CARNEIRO, Glauco. **História das revoluções brasileiras**. Rio de Janeiro: Record, 1989.

FAUSTO, Boris. **Getúlio Vargas**: o poder e o sorriso. São Paulo: Companhia das Letras, 2006.

HOBSBAWM, Eric. **A Era dos Extremos** – O Breve Século XX (1914-1991). São Paulo: Companhia das Letras, 1995.

MINISTÉRIO DA DEFESA. Estado-Maior do Exército. **Manual de Campanha Comando e Controle** - EB20-MC-10.205. Brasília, 2015.

MINISTÉRIO DA DEFESA. Estado-Maior do Exército. **Manual de Campanha Liderança Militar** - C-20.10. Brasília, 2011.

MINISTÉRIO DA DEFESA. Estado-Maior do Exército. **Manual de Fundamentos Doutrina Militar Terrestre** - EB20-MF-10.102. Brasília, 2019.

MOTTA, Rodrigo Patto Sá. **Em guarda contra o perigo vermelho**: o anticomunismo no Brasil (1917-1964). Niterói: Eduff, 2020.

REIS, Daniel Araão. **Luís Carlos Prestes**: um revolucionário entre dois mundos. São Paulo: Companhia das Letras, 2014.

TRESPACH, Rodrigo. **Histórias não (ou mal) contadas**: revoltas, golpes e revoluções no Brasil. Rio de Janeiro: Harper Colins, 2017.

VICENTINO, Cláudio; DORIGO, Gianpaolo. **História do Brasil**. 2. ed. atual. São Paulo: Scipione, 2009.

WAACK, William. **Camaradas**: nos arquivos de Moscou: a história secreta da revolução brasileira de 1935. São Paulo: Companhia das Letras, 1993.

---

i Estabelecimento de ligações de comunicações, normalmente feito por meio de radiofrequência, meios físicos, tais como cabos telefônicos ou óticos ou sinais visuais (Ministério da Defesa, 2015, p.1-3).
ii Waack, 1993, p.205.
iii Fausto, 2006, p.73.
iv Waack, 1993, p.44 e 212.
v Aragão, 1973, p.18.
vi Brasil. Presidência da República. Lei nº 38, de 4 de abril de 1935. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/1930-1949/l0038.htm>. Acesso em: 05 de ago. de 2024.
vii Motta, 2020, p.205-206.
viii Vicentino, 2009, p.361.
ix Aragão, 1973, p.48.
x Motta, 2020, p.208.
xiWaack, 1993, p.55.
xii Expressão utilizada pela primeira vez pelo general Isidoro Dias Lopes, em referência ao caráter mítico atribuído à chamada Coluna Prestes (Reis, 2014, p.110).
xiii Waack, 1993, p.157.

xiv Waack, 1993, p.225.
xv Motta, 2020, p.206.
xvi Waack, 1993, p.145 e p.198.
xvii Waack, 1993, p.156.
xviii Fausto, 2006, p.74.
xix Partido Comunista da União Soviética.
xx Em especial, as Considerações Civis (Ministério da Defesa, 2019, p.5-8).
xxi Reis, 2014, p.184.
xxii Ministério da Defesa, 2015, p. 1-2.
xxiii Motta, 2020, p.143.
xxiv Estilo de liderança caracterizado pela centralização das decisões pelo líder em detrimento do assessoramento dos subordinados. O C-20-10, "Manual de Campanha de Liderança Militar", aponta que, quando empregado indiscriminadamente e por tempo prolongado, a liderança autocrática tende a desgastar os vínculos afetivos entre o comandante e os comandados, bem como restringir capacidades e gerar resultados negativos para o atingimento das metas de um grupo.
xxv Ministério da Defesa, 2015, p.2-2.
xxvi Reis, 2014, p.182.
xxvii Waack, 1993, p.203.
xxviii Reis, 2014, p.188.
xxix Acrônimo em russo para Komitet Gosudarstvennoi Bezopasnosti, ou Comitê de Segurança do Estado.
xxx Trespach, 2017, p.163.
xxxi Ao menos segundo a versão fornecida pelas autoridades (Fausto, 2006, p.77).
xxxii Waack, 1993, p.300.
xxxiii Judia, Olga seria deportada para Alemanha, onde morreria, vítima do regime nazista, em uma câmara de gás.
xxxiv Motta, 2020, p.212.
xxxv Dentre os panfletos apreendidos, constam promessas de promoção e concessão de estabilidade aos sargentos, além de aumento dos salários. Ver Aragão, 1973, p.97.
xxxvi Como, por exemplo, no Quartel-General da 1ª Região Militar, onde o tenente Augusto Paes Barreto foi preso na noite de 26 enquanto anunciava aos subordinados que, a partir daquela data, Prestes liderava a transição do Brasil para um regime de caráter comunista. Ver Aragão, 1973, p.78.
xxxvii Motta, 2020, p.212.
xxxviii Ver: https://pcb.org.br/portal2/9846. Acesso em: 05 de ago. de 2024.
xxxix Entre as fontes referenciadas, o número varia de 100 a 720.
xl VÍTIMAS da Intentona Comunista de 1935 são rememoradas. TV CML, 2019. Disponível em: https://www.youtube.com/watch?v=Pu01vgtLHW8. Acesso em: 03 de ago. de 2024.
xli Aragão, 1973, p.139.

NSOC (Network Security Operation Center)

Sgt **PABLO PEREIRA** DA SILVA
Sgt **JAIME** DE MELO GAMA DA SILVA

***Resumo*—O objetivo principal do estudo sobre o NSOC (Network Security Operation Center) é desenvolver e implementar um centro de operações de segurança de rede usando ferramentas e tecnologias open-source como Zabbix, Pfsense, Snort, Vyos, Exos e GNS3. O objetivo do projeto é estabelecer um ambiente de monitoramento e resposta a incidentes cibernéticos que garantam a integridade, disponibilidade e confidencialidade dos ativos de rede da organização, detectando, analisando e mitigando ameaças em tempo real. As descobertas do estudo mostram que a implementação de um NSOC usando essas tecnologias de código aberto é viável e eficaz, oferecendo uma solução sólida para a segurança cibernética em redes corporativas. O novo sistema se destaca como uma ferramenta estratégica para proteger os ativos digitais, pois pode monitorar o tráfego de rede, descobrir problemas e responder rapidamente a incidentes. O uso de ferramentas open-source também permite uma personalização e escalabilidade maior do sistema, tornando-o uma opção viável para organizações que buscam melhorar sua postura de segurança cibernética sem comprometer o orçamento.**

***Palvras-chave*—NSOC. Zabbix. Pfsense. Snort. DMZ. Vyos. Exos. GNS3.**

***Abstract*— The main objective of the Network Security Operation Center (NSOC) study is to develop and implement a network security operations center using open-source tools and technologies such as Zabbix, Pfsense, Snort, Vyos, Exos, and GNS3. The goal of the project is to establish a cyber incident monitoring and response environment that ensures the integrity, availability, and confidentiality of the organization's network assets by detecting, analyzing, and mitigating threats in real time. The study's findings show that implementing an NSOC using these open-source technologies is feasible and effective, offering a solid solution for cyber security in corporate networks. The new system stands out as a strategic tool for protecting digital assets, as it can monitor network traffic, discover issues, and respond quickly to incidents. The use of open-source tools also allows for greater customization and scalability of the system, making it a viable option for organizations looking to improve their cyber security posture without compromising their budget.**

***Keywords*— NSOC. Zabbix. Pfsense. Snort. DMZ. Vyos. Exos. GNS3.**

I. Introdução

Uma instalação conhecida como centro de operações de segurança de rede (NSOC) abriga uma equipe de segurança da informação que monitora e avalia regularmente a posição de segurança de uma organização [1].

O objetivo da equipe do NSOC é detectar, analisar e responder os incidentes de segurança cibernética usando uma série de processos e soluções tecnológicas. Em geral, os centros de operações de segurança têm analistas e engenheiros de segurança, além de gerentes que supervisionam os procedimentos de segurança [2].

A equipe do NSOC trabalha em conjunto com as equipes de resposta a incidentes para garantir que os problemas de segurança sejam resolvidos rapidamente durante e/ou após a descoberta. Os centros de operações de segurança monitoram e analisam as atividades dos ativos de suas redes, como servidores, terminais de usuários, bancos de dados, aplicativos, sites e outros sistemas, para detectar incidentes ou ativos comprometidos [3].

Neste projeto, propomos a criação de um NSOC (Network Security Operations Center) utilizando o simulador de redes GNS3. Para a construção desse NSOC, serão empregados dis- positivos como roteadores Vyos e Exos, além de ferramentas como Zabbix e Pfsense.

II.Referencial Teórico

Registrar pacotes com facilidade. Ele também pode registrar pacotes do protocolo de controle de transmissão TCP. Ele é um sistema sofisticado de prevenção à intrusão, registrador de pacotes e sniffer de pacotes. A análise de protocolo pode detectar ataques de buffer overflow, stealth port scans, ataques CGI, SMB probes, identificação do sistema operacional, entre outros ataques [13].

A.Zabbix

O Zabbix [4] é uma ferramenta de monitoramento de código aberto projetada para monitorar a infraestrutura de rede. Ele pode monitorar redes, servidores, máquinas virtuais e serviços em nuvem. Essa ferramenta funciona para o monitoramento convencional e monitoramento de serviços simples sem a necessidade do uso de agentes, possui suporte nativo ao protocolo SNMP e disponibiliza uma interface web para a administração e monitoramento dos dados, onde pode ser configurado alertas de sistema para comunicação com o gerenciador da rede [5].

A coleta de dados, a ativação de triggers e o envio de notificações aos usuários são feitos pelo componente central da gerência do Zabbix. Os agentes e proxys que monitoramos dispositivos fornecem informações ao servidor Zabbix. A instalação deste servidor deve ocorrer em sistemas Unix ou Linux [6].

Zabbix Proxy é uma ferramenta que pode ser usada de forma opcional para monitorar e centralizar dados em infraestrutura de TI de forma remota. Ele transmite os dados coletados parao servidor Zabbix. O agente Zabbix é instalado nos hosts e pode usar scripts para capturar métricas como uso de CPU, memória e métricas personalizadas. É com base nesses dados que você pode criar gráficos personalizados para o usuário [7].

B. Pfsense

O pfsense [8], baseado no FreeBSD e projetado para funcionar tanto como firewall quanto como roteador, é um dos firewalls opensource mais conceituados e robustos disponíveis no mercado atualmente.

O pfsense é um firewall baseado em software que protege a rede monitorando o tráfego de entrada e saída e tomando decisões de permitir ou bloquear tráfego específico de acordo com as regras de segurança definidas [9].

Uma das principais vantagens de usar o pfsense é que ele é Open Source, estável, leve e possui uma licença de código aberto. Além disso, ele não exige hardware muito grande. Ele possui algumas características que facilitam a utilização, como uma interface WEB fácil de usar, uma grande variedade de pacotes de software, visualização de ambiente em tempo real e gerenciamento de ameaças unificadas [10].

C. Snort

A segurança da informação é um componente crucial do monitoramento de tráfego em uma rede de computadores. O Snort [11] é um IDS (Sistema de detecção de intrusão) bem conhecido e amplamente utilizado porque não requer muito poder de processamento e é fornecido como software livre, gratuito e mantido pela Cisco via rede [12].

O Snort se destaca por analisar tráfegos em tempo real e registrar pacotes com facilidade. Ele também pode registrar pacotes do protocolo de controle de transmissão TCP. Ele é um sistema sofisticado de prevenção à intrusão, registrador de pacotes e sniffer de pacotes. A análise de protocolo pode detectar ataques de buffer overflow, stealth port scans, ataques CGI, SMB probes, identificação do sistema operacional, entre outros ataques [13].

D. SNMP versão 3

O protocolo padrão chamado Simple Network Management Protocol (SNMP) é usado para gerenciar dispositivos em redes de computadores e na internet. Existem várias versões do SNMP, mas as 2c (SNMPv2c) e 3 (SNMPv3) são as mais usadas. O SNMPv3 é o mais recente e seguro. Foi introduzido para corrigir os problemas de segurança encontrados nas versões anteriores do protocolo [14]. O SNMPv3 tem as seguintes características principais:

- Autenticação: A SNMPv3 suporta forte autenticação, o que significa que as mensagens SNMP são autenticadas para garantir que são enviadas por uma fonte confiável. O HMAC-MD5-96 e o HMAC-SHA-96 são métodos de validação.
- Privacidade (Criptografia): É possível criptografar as mensagens SNMP para proteger os dados durante a transmissão. Isso é executado principalmente com o protocolo DES, mas pode também suportar o AES.

- Controle de Acesso: A SNMPv3 inclui controles de acesso mais complexos, o que permite que os administra- dores configurem permissões específicas para quem podeacessar informações em um dispositivo de rede.

Por fim, a SNMPv3 é recomendada para ambientes com altos requisitos de segurança devido às suas capacidades avançadas de autenticação e criptografia, enquanto a SNMPv2cpode ser usada em ambientes menos críticos onde a compati- bilidade e a simplicidade são mais importantes [15].

III. METODOLOGIA

Para a construção da topologia deste trabalho, utilizou- se o simulador GNS3 [16]. No GNS3, foram empregadas appliances de roteadores VyOS e Exos, ferramentas do PfSense e do Zabbix, sistemas operacionais Ubuntu 18.04 e Kali Linux, além das appliances nativas do GNS3, como modem, switch e VPCS.

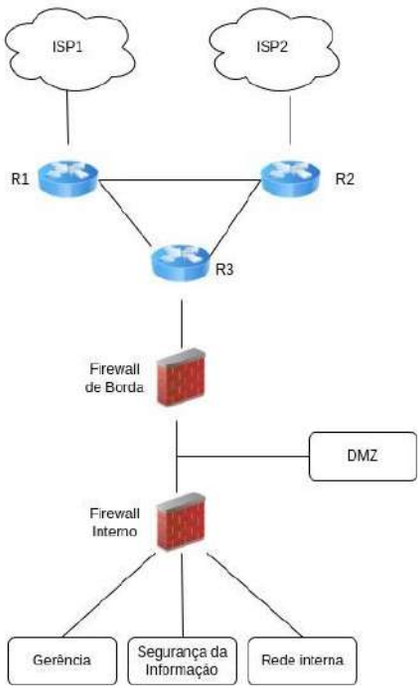
O trabalho foi desenvolvido utilizando uma metodologia científica que combina pesquisa aplicada, metodologia experimental, estudo de caso, e simulação. Usando ferramentas de código aberto em um ambiente simulado, o estudo se concentrou na implementação prática e avaliação de um Network Security Operation Center (NSOC). A técnica experimental permitiu o teste de algumas configurações e a análise da eficácia das tecnologias usadas para detectar e proteger ameaças cibernéticas. Além disso, uma pesquisa de desenvolvimento tecnológico ajudou a desenvolver soluções úteis para monitoramento e segurança de redes [17].

IV. TOPOLOGIA

A topologia proposta é ilustrada na Figura 1, sendo composta por um Backbone de ISPs, uma área DMZ, uma área de Gerência, uma área de Segurança da Informação e uma Rede Interna. A estrutura também inclui dois firewalls: um firewall de borda e um firewall interno.

Para simular essa topologia, foi utilizado o software GNS3. O GNS3 (Graphical Network Simulator-3) uma ferramenta de simulação de redes que permite a criação e teste de topologias de rede. Ele oferece uma interface gráfica que facilita a configuração e o gerenciamento de dispositivos de rede, como roteadores, switches e firewalls, possibilitando simulações em um ambiente controlado. A topologia proposta no GNS3 está exposta na Figura 2

Figura 1: Topologia Proposta



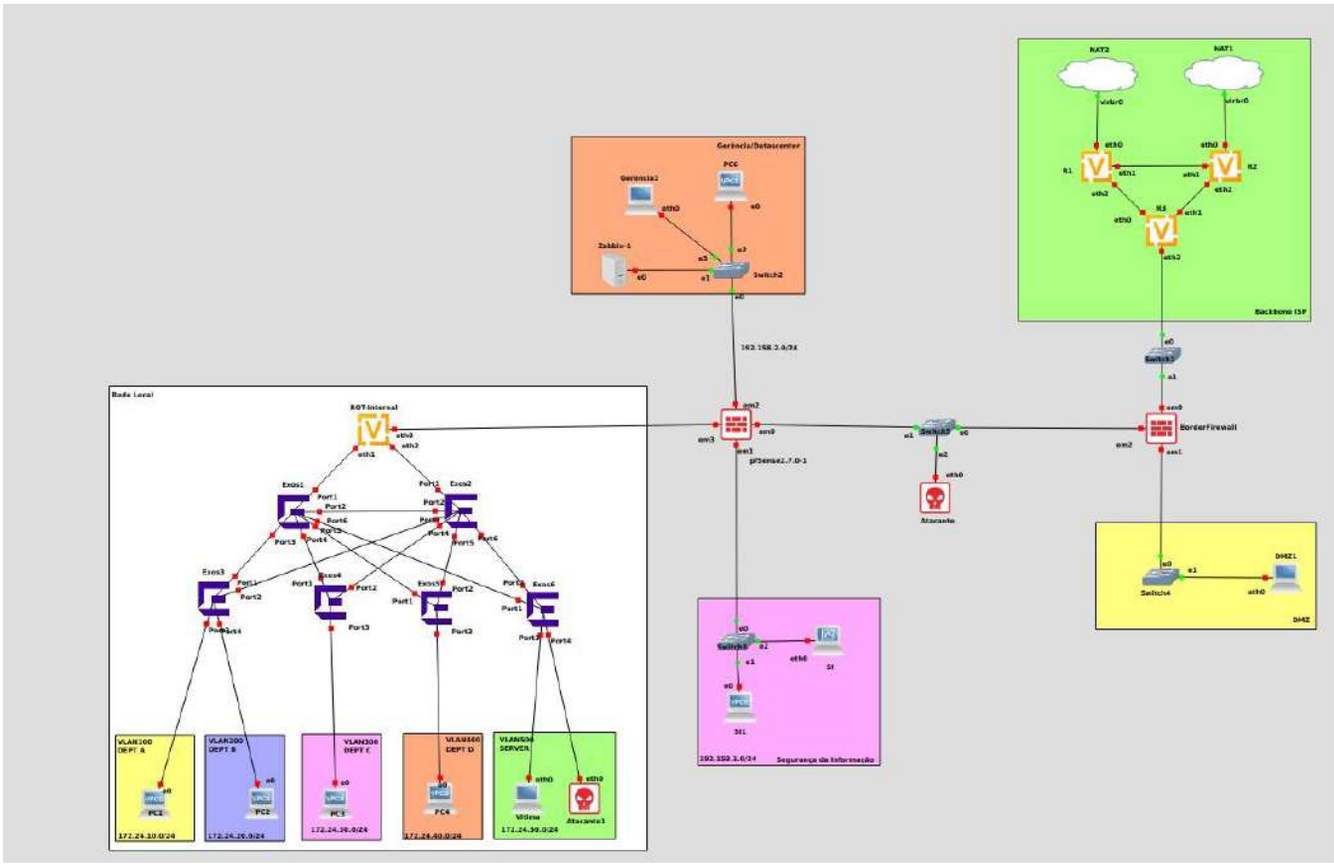


Figura 2: Topologia Proposta No GNS3

V. Backbone de Provedores de Internet

Foi criada uma área de simulação de provedores de internet, que inclui duas nuvens NAT e três roteadores VyOS. A utilização de duas nuvens NAT visa proporcionar redundância de rede, garantindo maior confiabilidade e disponibilidade dos serviços.

Essa será a área responsável por prover acesso à internet para todos os dispositivos da topologia. Em uma rede, os provedores de internet (ISPs - Internet Service Providers) são entidades que oferecem serviços de conectividade à internet para usuários finais, empresas e outras organizações.

A área utiliza o intervalo de IP 192.168.15.0/24 como base. Os IPs atribuídos a cada interface podem ser visualizados na Tabela I.

Dispositivo	Interface	IP/Máscara
R1	eth0 eth1 eth2	via DHCP Nuvem 192.168.15.1/28 192.168.15.17/28
R2	eth0 eth1 eth2	via DHCP nuvem 192.168.15.14/28 192.168.15.33/28
R3	eth0 eth1 eth2	192.168.15.30/28 192.168.15.46/28 192.168.15.49/28

Tabela I: Tabela de roteadores da área de provedores

Para a distribuição de rotas, foi configurado o protocolo OSPF em todos os roteadores da área de provedores. A utilização do OSPF (Open Shortest Path First) elimina a necessidade de cadastrar manualmente as rotas entre os roteadores, simplificando a administração da rede.

A configuração do OSPF no roteador R1 pode ser visualizada na Figura 3, enquanto a sua tabela de roteamento está apresentada na Figura 4.

A configuração do OSPF no roteador R2 pode ser visualizada na Figura 5, enquanto a sua tabela de roteamento está apresentada na Figura 6.

A configuração do OSPF no roteador R3 pode ser visualizada na Figura 7, enquanto a sua tabela de roteamento está apresentada na Figura 8.

No roteador R3, foi configurado um servidor DHCP na interface eth3 para que o firewall de borda pudesse receber automaticamente o IP e o gateway dessa sub-rede. Isso elimina a necessidade de configurar manualmente os endereços IP e os gateways nos dispositivos conectados. Além disso, garante uma configuração consistente e correta, reduzindo a probabilidade de erros de configuração.

Para testar a redundância dos ISPs, foi realizado um teste de ping no servidor gns3 com o endereço IP 192.168.122.1. Inicialmente, verificou-se que, no roteador R3, a rota utilizada passava pelo roteador R2. Para validar a funcionalidade da

```
vyos@vyos# show protocols ospf
 area 0 {
     network 192.168.122.0/24
     network 192.168.15.0/28
     network 192.168.15.16/28
 }
 default-information {
     originate {
         metric 10
         metric-type 2
     }
 }
 log-adjacency-changes {
 }
 parameters {
     router-id 10.1.1.1
 }
 redistribute {
     connected {
         metric-type 2
         route-map CONNECT
     }
 }
[edit]
vyos@vyos#
```

Figura 3: Configuração do OSPF do roteador R1

```
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 0.0.0.0/0 [110/10] via 192.168.122.1, eth0, 00:05:06
S   0.0.0.0/0 [210/0] via 192.168.122.1, eth0, 00:06:07
C>* 10.1.1.1/32 is directly connected, lo, 00:06:12
O>* 10.2.2.2/32 [110/20] via 192.168.15.14, eth1, 00:05:06
  *                      via 192.168.122.160, eth0, 00:05:06
O>* 10.3.3.3/32 [110/20] via 192.168.15.30, eth2, 00:04:23
O   192.168.15.0/28 [110/100] is directly connected, eth1, 00:06:16
C>* 192.168.15.0/28 is directly connected, eth1, 00:06:12
O   192.168.15.16/28 [110/100] is directly connected, eth2, 00:06:10
C>* 192.168.15.16/28 is directly connected, eth2, 00:06:11
O>* 192.168.15.32/28 [110/200] via 192.168.15.14, eth1, 00:04:24
  *                            via 192.168.15.30, eth2, 00:04:24
  *                            via 192.168.122.160, eth0, 00:04:24
O>* 192.168.15.48/28 [110/200] via 192.168.15.30, eth2, 00:04:24
O   192.168.122.0/24 [110/100] is directly connected, eth0, 00:05:07
C>* 192.168.122.0/24 is directly connected, eth0, 00:06:08
```

Figura 4: Tabela de Roteamento do roteador R1

```
vyos@vyos# show protocols ospf
 area 0 {
     network 192.168.122.0/24
     network 192.168.15.0/28
     network 192.168.15.32/28
 }
 default-information {
     originate {
         metric 10
         metric-type 2
     }
 }
 log-adjacency-changes {
 }
 parameters {
     router-id 10.2.2.2
 }
 redistribute {
     connected {
         metric-type 2
         route-map CONNECT
     }
 }
[edit]
vyos@vyos#
```

Figura 5: Configuração do OSPF do roteador R2

```
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 0.0.0.0/0 [110/10] via 192.168.122.1, eth0, 00:13:26
S   0.0.0.0/0 [210/0] via 192.168.122.1, eth0, 00:14:08
O>* 10.1.1.1/32 [110/20] via 192.168.15.1, eth1, 00:13:20
  *                     via 192.168.122.38, eth0, 00:13:20
C>* 10.2.2.2/32 is directly connected, lo, 00:14:12
O>* 10.3.3.3/32 [110/20] via 192.168.15.46, eth2, 00:12:44
O   192.168.15.0/28 [110/100] is directly connected, eth1, 00:14:11
C>* 192.168.15.0/28 is directly connected, eth1, 00:14:12
O>* 192.168.15.16/28 [110/200] via 192.168.15.1, eth1, 00:12:45
  *                            via 192.168.15.46, eth2, 00:12:45
  *                            via 192.168.122.38, eth0, 00:12:45
O   192.168.15.32/28 [110/100] is directly connected, eth2, 00:14:11
C>* 192.168.15.32/28 is directly connected, eth2, 00:14:12
O>* 192.168.15.48/28 [110/200] via 192.168.15.46, eth2, 00:12:45
O   192.168.122.0/24 [110/100] is directly connected, eth0, 00:14:08
C>* 192.168.122.0/24 is directly connected, eth0, 00:14:08
```

Figura 6: Tabela de Roteamento do roteador R2

```
vyos@vyos# show protocols ospf
 area 0 {
     network 192.168.15.16/28
     network 192.168.15.32/28
     network 192.168.15.48/28
 }
 default-information {
     originate {
         metric 10
         metric-type 2
     }
 }
 log-adjacency-changes {
 }
 parameters {
     abr-type cisco
     router-id 10.3.3.3
 }
 redistribute {
     connected {
         metric-type 2
         route-map CONNECT
     }
 }
[edit]
vyos@vyos#
```

Figura 7: Configuração do OSPF do roteador R3

```
vyos@vyos:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

O>* 0.0.0.0/0 [110/10] via 192.168.15.17, eth0, 00:13:56
  *                    via 192.168.15.33, eth1, 00:13:56
O>* 10.1.1.1/32 [110/20] via 192.168.15.17, eth0, 00:13:56
O>* 10.2.2.2/32 [110/20] via 192.168.15.33, eth1, 00:14:00
C>* 10.3.3.3/32 is directly connected, lo, 00:14:20
O>* 192.168.15.0/28 [110/200] via 192.168.15.17, eth0, 00:13:57
  *                           via 192.168.15.33, eth1, 00:13:57
O   192.168.15.16/28 [110/100] is directly connected, eth0, 00:14:06
C>* 192.168.15.16/28 is directly connected, eth0, 00:14:16
O   192.168.15.32/28 [110/100] is directly connected, eth1, 00:14:01
C>* 192.168.15.32/28 is directly connected, eth1, 00:14:17
O   192.168.15.48/28 [110/100] is directly connected, eth2, 00:14:17
C>* 192.168.15.48/28 is directly connected, eth2, 00:14:17
O>* 192.168.122.0/24 [110/200] via 192.168.15.17, eth0, 00:13:57
  *                            via 192.168.15.33, eth1, 00:13:57
vyos@vyos:~$
```

Figura 8: Tabela de Roteamento do roteador R3

redundância, o roteador R2 foi pausado, forçando o roteador R3 a encontrar uma rota alternativa através do roteador R1, conforme mostrado na Figura 9.

A. SNMP versão 3 no Vyos

Para que a equipe de gerência pudesse administrar corretamente todos os dispositivos necessários da topologia, foi necessário configurar o protocolo SNMPv3 nos roteadores. Como todos os roteadores são VyOS, a configuração foi a mesma em todos os dispositivos, alterando apenas os IPs. Uma demonstraçao da configuração pode ser visto no Código 1.

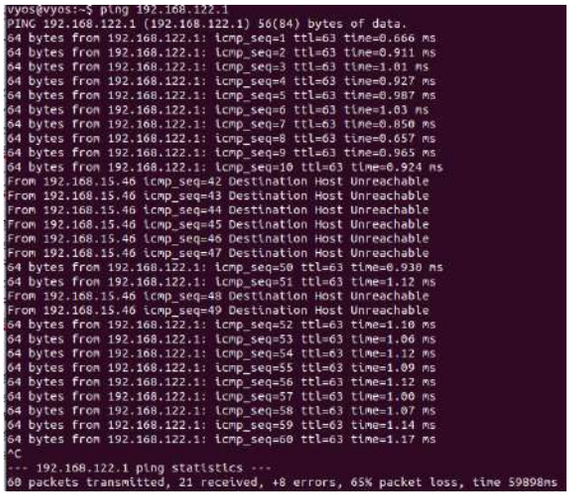


Figura 9: Ping para teste da redundância de ISPs

```
set service snmp listen-address 192.168.15.1
set service snmp listen-address 192.168.15.17
set service snmp location 'VyosISP'
set service snmp v3 engineid '00000000000000000000000002'
set service snmp v3 view snmpview1 oid 1
set service snmp v3 group vyosgroup mode ro
set service snmp v3 group vyosgroup seclevel priv
set service snmp v3 group vyosgroup view snmpview1
set service snmp v3 user vyos auth plaintext-key seglannajaime
set service snmp v3 user vyos auth type 'sha'
set service snmp v3 user vyos group vyosgroup
set service snmp v3 user vyos privacy plaintext-key seglannajaime
set service snmp v3 user vyos privacy type 'aes'
```

Código 1: Configuração do SNMP versão 3 no Vyos

Para a configuração do SNMPv3, foi criado um grupo chamado "vyosgroup", associado ao OID 1. O OID (Object Identifier) é um identificador usado para especificar uma determinada variável ou objeto gerenciado na MIB (Management Information Base).

O grupo "vyosgroup"foi configurado no modo "ro"(read-only), o que significa que os usuários deste grupo têm permissão apenas para ler informações dos dispositivos gerenciados.

Além disso, o grupo foi configurado com autenticação SHA (Secure Hash Algorithm) e privacidade AES (Advanced Encryption Standard). A autenticação SHA garante que apenas usuários autorizados possam acessar o dispositivo, enquanto a privacidade AES criptografa os dados transmitidos, protegendo contra interceptações e garantindo a confidencialidade das informações.

Esse padrão de configuração do SNMPv3 foi seguido em toda a topologia.

VI. Firewall de Borda

O firewall de borda é importante para a segurança de uma rede. Ele atua como a primeira linha de defesa contra ameaças externas, bloqueando tráfego malicioso e impedindo tentativas de invasão. Além disso, o firewall regula o tráfego de entrada e saída, permitindo apenas o acesso autorizado aos recursos da rede e impedindo acessos não autorizados.

O pfSense foi escolhido como firewall de borda nesta topologia, pois ele oferece recursos como prevenção e detecção de intrusões (IDS/IPS), VPNs para conexões seguras, e filtragem de conteúdo, além de possuir uma interface web que facilita a administração.

Foram utilizadas três interfaces no firewall de borda: a interface em0 conecta-se à área de ISPs, a interface em1 liga-se à área DMZ, e a interface em2 estabelece conexãocom o firewall interno. Os IPs do firewall de borda pode ser visualizada na Figura 10.

Figura 10: Configuração dos IPs do Firewall de Borda

A interface em0 recebe seu IP através do servidor DHCP do roteador R3 da área de provedores. As demais interfaces possuem endereços IP na faixa 192.168.0.0/16. Especificamente, a interface em1 está configurada na subrede 192.168.1.0/24, enquanto a interface em2 está na subrede 192.168.2.0/24.

As interfaces em1 e em2 também possuem servidores DHCP configurados. Isso permite que essas interfaces atribuam automaticamente endereços IP a dispositivos conectados a elas.

Para configurar o DHCP no pfSense, é preciso acessar a guia *Services -> DHCP Server* e selecionar a interface desejada. Em seguida, é necessário informar o intervalo de IPs disponíveis para serem atribuídos aos dispositivos da rede. Isso permite que o pfSense gerencie dinamicamente a atribuição de endereços IP dentro desse intervalo.

Embora não tenham sido configuradas regras de firewall para as interfaces do firewall de borda, é importante notar que a área da DMZ funciona de forma isolada, sem qualquer conhecimento da rede interna, que inclui as áreas de gerência, segurança da informação e rede local. Essa estratégia de isolamento garante a segurança da rede interna, protegendo-a de possíveis ameaças que possam surgir na DMZ. Ao restringir o acesso direto da DMZ à rede interna, diminui a superfície de ataque e os riscos a infraestrutura interna.

A. SNMP versão 3 no Pfsense

No pfSense, foi possível habilitar e configurar o protocolo SNMPv3 através da instalação de um pacote externo chamado "net-snmp", configurado para utilizar o protocolo UDP na porta 161.

Assim como no VyOS, foi configurado um usuário com permissões de leitura apenas (read-only), utilizando autenticação SHA e privacidade AES, como mostra a Figura 11.

É importante ressaltar que, para que este pacote funcione corretamente, o serviço SNMP nativo do pfSense deve ser desabilitado.

B. Sistemas de prevenção e detecção de intrusão

Para a detecção e prevenção de intrusões, foi implementado o Snort no firewall de borda. O Snort é um sistema capaz de monitorar o tráfego de rede em tempo real, identificar padrões suspeitos ou maliciosos e tomar medidas para mitigar possíveis ameaças.

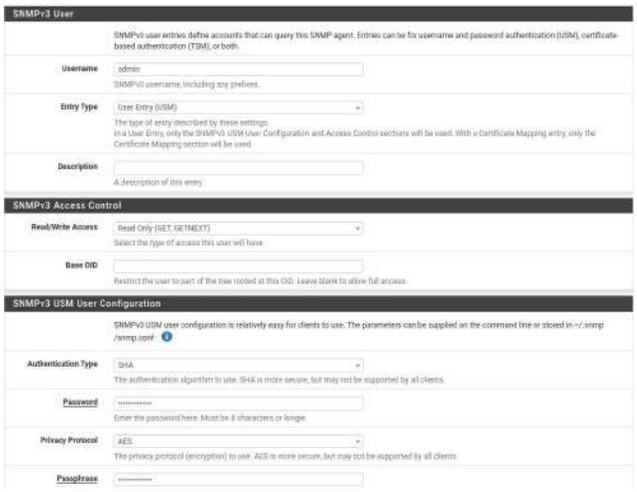


Figura 11: Configuração do SNMPv3 no pfsense

O Snort não é uma ferramenta nativa no pfSense, sendo necessário instalá-lo através do Gerenciador de Pacotes disponível, com o nome "snort". Além disso, para utilizar o pacote, é necessário obter um código do Snort Oinkmaster, que pode ser adquirido na página oficial do Snort.

O Snort foi habilitado nas três interfaces ativas do firewall de borda, com mostra a Figura 12. As configurações padrão do pfSense já constituem um IDS. Para habilitar o IPS, é necessário, nas configurações de interface, ativar as opções "Block Offender"e "Kill States". Isso fará com que, ao detectar um alerta, o Snort bloqueie o host e rejeite a comunicação.

Figura 12: Configuração do Snort nas Interfaces

Por padrão, muitos IPs são bloqueados pelo IPS, incluindo os IPs associados aos pacotes do Ubuntu e do Python, como mostra Figura.13. Supondo que existam desenvolvedores python nas áreas da topologia, foi necessário criar uma lista de permissões (whitelist) contendo o IP do pyhosted.org, permitindo que os desenvolvedores acessem e baixem bibliotecas Python via pip. Isso garante que o acesso aos recursos necessários seja concedido de forma segura, enquanto mantém a integridade e a segurança da rede.

Deve-se incluir os IPs necessários para o funcionamento e desenvolvimento nas áreas específicas da topologia na lista de permissões (pass list) do Snort, garantindo que esses IPs não sejam bloqueados pelo sistema de prevenção de intrusões. Isso assegura que o tráfego legítimo relacionado às atividades de operação e desenvolvimento da rede não seja interrompido, enquanto se mantém a segurança e a integridade do ambiente de rede.

Figura 13: pyhosted.org sendo bloquado pelo IPS do Snort

VII. Firewall Interno

Enquanto o firewall de borda protege a rede como um todo contra ameaças externas, o firewall interno é usado para garantir a segurança dentro da própria rede, controlando o tráfego entre diferentes partes da infraestrutura interna.

O firewall interno é posicionado dentro da rede interna, aplicando políticas de segurança específicas para diferentes grupos de usuários e dispositivos, ele é utilizado para segmentar a rede interna e controlar o tráfego entre diferentes partes da infraestrutura interna.

O pfSense também foi escolhido como firewall interno nesta configuração. A interface em0 está conectada ao firewall externo, a interface em1 está ligada à área de segurança da informação, a interface em2 está conectada à área de gerência e a interface em3 está conectada à área de rede local. A tabela de IPs correspondente pode ser visualizada na Figura 14.

Figura 14: Configuração dos IPs do Firewall Interno

A interface em0 recebe seu IP através do servidor DHCP do firewall de borda. As demais interfaces possuem endereços IP na faixa 192.158.0.0/16. Especificamente, a interface em1 está configurada na subrede 192.158.1.0/24, a interface em2 está na subrede 192.158.2.0/24, enquanto a interface em3 está na subrede 192.158.3.0/24.

As interfaces em1, em2 e em3 possuem servidores DHCP configurados. Isso permite que essas interfaces atribuam automaticamente endereços IP a dispositivos conectados a elas.

O protocolo SNMPv3 também foi configurado no firewall interno, utilizando as mesmas configurações aplicadas no firewall de borda, conforme descrito na subseção VI-A.

A. Regras do firewall interno

Para o controle de tráfego da rede, foram estabelecidas algumas regras de segurança no firewall interno:

- A área de gerência terá acesso a toda a topologia.
- Nenhuma outra área terá permissão para acessar a área de gerência.
- A área de rede local não terá acesso à área de segurança da informação.

Essas regras foram implementadas para garantir a integridade e a segurança da rede, limitando o acesso apenas as áreas autorizados e impedindo comunicações não autorizadas entre áreas específicas da infraestrutura. Essas configurações podem ser vizualizadas na Figura 15.

Para permitir que a área de gerência possa acessar os departamentos da rede local, foi necessário configurar uma rota estática no firewall interno. Essa rota encaminha todo o tráfego destinado à rede 172.24.0.0/16 para o gateway 192.168.3.10, que é o endereço associado à interface eth0 do ROT-Internal.

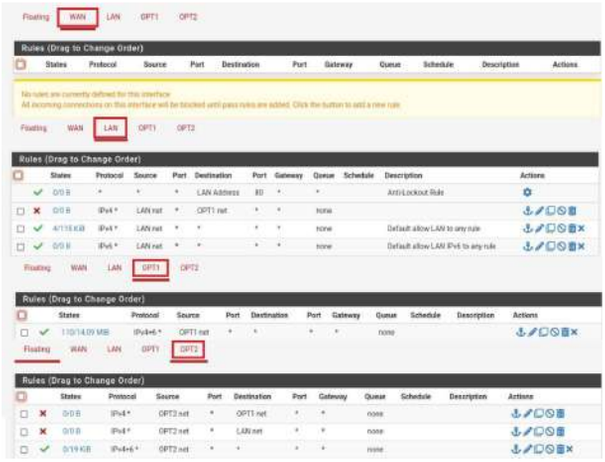


Figura 15: Configuração das regras no firewall interno

VIII. Rede Local

A área nomeada como rede local, é onde estão os diferentes departamentos ou setores de uma organização, simulando um ambiente de trabalho interno. Nessa topologia, cada departamento pode ser considerado uma subdivisão da rede local, com suas próprias necessidades de comunicação e segurança.

Foi implementado um backbone da rede local com redundância, utilizando 1 roteador VyOS e 2 dispositivos Exos, que operam na camada de rede 3, desempenhando o papel de roteadores. Essa configuração visa garantir alta disponibilidade e tolerância a falhas na infraestrutura de rede local.

Foram implementados também 4 dispositivos Exos que operam na camada de rede 2, desempenhando a função de switches.

Os três dispositivos que atuam como roteadores na rede local têm o protocolo OSPF configurado. Além disso, os dois roteadores Exos também têm o protocolo DHCP configurado, permitindo que os usuários dos departamentos da topologia recebam endereços IP automaticamente.

A rede base utilizada nas VLANs do backbone e nos departamentos da rede interna possui o endereço IP base 172.24.0.0/16. Para configurar e conectar o VyOS com os Exos, foi necessário criar VLANs.

A configuração das VLANs no ROT-Internal pode ser vista na Figura 16, enquanto a configuração das VLANs no Exos1 e Exos2 pode ser visualizada nas Figuras 17 e 18, respectivamente.

```
vyos@vyos:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet 10.4.4.4/32 scope global lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 0c:73:8c:9c:00:00 brd ff:ff:ff:ff:ff:ff
    inet 192.158.3.10/24 brd 192.158.3.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::e73:8cff:fe9c:0/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 0c:73:8c:9c:00:01 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::e73:8cff:fe9c:1/64 scope link
       valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 0c:73:8c:9c:00:02 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::e73:8cff:fe9c:2/64 scope link
       valid_lft forever preferred_lft forever
5: eth2.12@eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state
UP group default qlen 1000
    link/ether 0c:73:8c:9c:00:02 brd ff:ff:ff:ff:ff:ff
    inet 172.24.1.1/24 brd 172.24.1.255 scope global eth2.12
       valid_lft forever preferred_lft forever
    inet6 fe80::e73:8cff:fe9c:2/64 scope link
       valid_lft forever preferred_lft forever
6: eth1.10@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state
UP group default qlen 1000
    link/ether 0c:73:8c:9c:00:01 brd ff:ff:ff:ff:ff:ff
    inet 172.24.0.1/24 brd 172.24.0.255 scope global eth1.10
       valid_lft forever preferred_lft forever
    inet6 fe80::e73:8cff:fe9c:1/64 scope link
       valid_lft forever preferred_lft forever
vyos@vyos:~$
```

Figura 16: Configuração dos IPs do ROT-Internal

```
* EXOS-VM.54 # show vlan
Untagged ports auto-move: Inform

Name            VID  Protocol Addr       Flags                        Proto  Ports  Virtual
                                                                              Active router
                                                                              /Total
--------------------------------------------------------------------------------------------
Default         1    ----------------------------------T-------------  ANY    0 /0   VR-Default
DEPTA           100  172.24.10.1    /24  -fL------o----------------  ANY    1 /1   VR-Default
DEPTB           200  172.24.20.1    /24  -fL------o----------------  ANY    1 /1   VR-Default
DEPTC           300  172.24.30.1    /24  -fL------o----------------  ANY    1 /1   VR-Default
DEPTD           400  172.24.40.1    /24  -fL------o----------------  ANY    1 /1   VR-Default
Mgnt            4095 ----------------------------------------------  ANY    0 /1   VR-Mgmt
SERVER          500  172.24.50.1    /24  -fL------o----------------  ANY    1 /1   VR-Default
VLANIF0         10   172.24.0.2     /24  -fL------o----------------  ANY    1 /1   VR-Default
VLANIF2         12   172.24.2.1     /24  -fL------o----------------  ANY    1 /1   VR-Default
--------------------------------------------------------------------------------------------
```

Figura 17: Configuração dos IPs do Exos1

```
* EXOS-VM.53 # show vlan
Untagged ports auto-move: Inform

Name            VID  Protocol Addr       Flags                        Proto  Ports  Virtual
                                                                              Active router
                                                                              /Total
--------------------------------------------------------------------------------------------
Default         1    ----------------------------------T-------------  ANY    0 /0   VR-Default
DEPTA           100  172.24.10.2    /24  -fL------o----------------  ANY    1 /1   VR-Default
DEPTB           200  172.24.20.2    /24  -fL------o----------------  ANY    1 /1   VR-Default
DEPTC           300  172.24.30.2    /24  -fL------o----------------  ANY    1 /1   VR-Default
DEPTD           400  172.24.40.2    /24  -fL------o----------------  ANY    1 /1   VR-Default
Mgnt            4095 ----------------------------------------------  ANY    0 /1   VR-Mgmt
SERVER          500  172.24.50.2    /24  -fL------o----------------  ANY    1 /1   VR-Default
VLANIF1         11   172.24.1.2     /24  -fL------o----------------  ANY    1 /1   VR-Default
VLANIF2         12   172.24.2.2     /24  -fL------o----------------  ANY    1 /1   VR-Default
--------------------------------------------------------------------------------------------
```

Figura 18: Configuração dos IPs do Exos2

A. SNMPv3 no Exos

A configuração do SNMPv3 no Exos seguiu o mesmo padrão já utilizado nos roteadores VyOS e no pfSense. Um usuário foi criado, com autenticação SHA e privacidade AES habilitadas, conforme ilustrado no Código 2.

```
configure snmpv3 add user exosuser authentication sha seglannajaime priv
aes seglannajaime

configure snmpv3 add group exosgroup user exosuser sec -model usm

configure snmpv3 add access exosgroup sec -model usm sec -level priv
read -view default Admin View write -view default Admin View notify -view default Admin View

enable snmp access snmpv3
```

Código 2: Configuração do SNMP versão 3 no Exos

A configuração foi realizada nos dois dispositivos Exos que operam na camada 3, não sendo necessária nos Exos que funcionam apenas como switches.

IX. DATASCENTER/GERÊNCIA

A área de gerência de redes é onde será feito o monitoramento e controle dos dispositivos e serviços da topologia. Para isso, será utilizado o Zabbix, que supervisiona o desempenho da rede, detecta e soluciona problemas, além de garantir a segurança.

Para descobrir todos os dispositivos da topologia, é necessário configurar o protocolo SNMPv3 em todos os dispositivos relevantes.

Para a busca dinâmica dos dispositivos no Zabbix, é necessário configurar regras de descoberta na aba Configuration -> Discovery. Foram cadastradas três regras: a primeira para encontrar os dispositivos conectados ao firewall de borda, a segunda para encontrar os dispositivos conectados ao firewall interno, e a terceira para encontrar os dispositivos da rede local, conforme mostrado na Figura 19. Para cada regra, foi informado os ranges de IPs que deveriam ser procurados.

Figura 19: Configuração das regras de descoberta no Zabbix

Para maior automação, também foram criadas ações de descoberta (Actions) no Zabbix, permitindo a adição automática desses hosts encontrados aos grupos de hosts escolhidos, especificando novamente os intervalos de IP necessários, como mostra a Figura 20

Figura 20: Configuração das Actions no Zabbix

Isso permitiu, através dos grupos de hosts criados, a criação do mapa da topologia, que foi simplificado para melhor visualização, conforme mostrado na Figura 21.

É importante notar que nem todos os dispositivos da topologia possuem o protocolo SNMPv2 ou v3 configurado, como, por exemplo, os computadores com Ubuntu.

Para monitorar as interfaces dos dispositivos, é necessário configurar o protocolo SNMPv3 em todos os hosts relevantes. Um exemplo dessa configuração no Zabbix pode ser visualizado na Figura 22.

Figura 21: Mapa da topologia no Zabbix

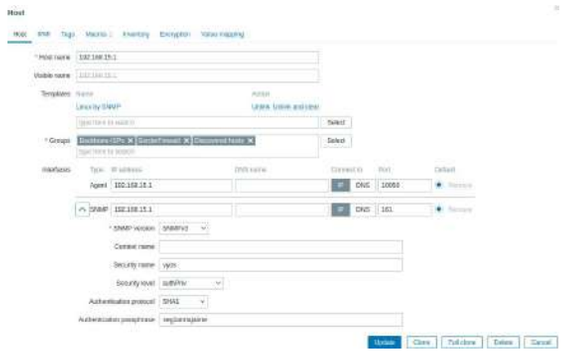


Figura 22: Exemplo de configuração do SNMPv3 nos hosts do Zabbix

O template do Zabbix, que é um conjunto pré-configurado de itens, gráficos e ações de monitoramento aplicáveis a múltiplos hosts, o escolhido para todos os hosts foi o "Linux by SNMP". Este template foi selecionado por oferecer bons gráficos e dashboards, que exibem informações como espaço de disco utilizado e tráfego de rede em todas as interfaces. Exemplos dos gráficos gerados para os hosts gerenciados podem ser visualizados nas Figuras 23 e 24.

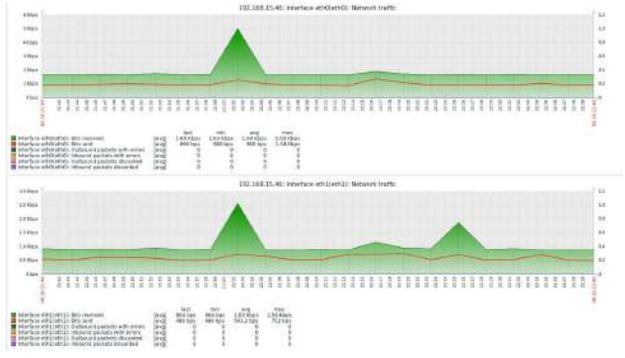


Figura 23: Exemplo das informações de tráfego de rede no Zabbix

X. DMZ

A DMZ (Demilitarized Zone) é uma área de rede que fica entre a rede interna de uma organização e a internet externa. Essa zona é criada para fornecer uma camada adicional de

Figura 24: Exemplo das informações de espaço em disco no Zabbix

segurança, segregando os sistemas críticos da rede interna daqueles acessíveis ao público externo.

Na DMZ, foi hospedada uma API REST utilizando o framework FastAPI, que simula uma API com autenticação para fins de teste. O código dessa API pode ser encontrado em [18]. Foi hospedado também um site HTTP com um formulário de login simples e seu código pode ser encontrado em [19].

Além disso, foi instalado um servidor SSH com o OpenSSH Server para simular um servidor acessível remotamente.

XI. Ataques e Vulnerabilidades Exploradas

Para simulação dos ataques foram usados máquinas com sistema kali linux. A localização dos atacantes na topologia pode ser visualizado na figura 2.

A. DHCP

O servidor DHCP foi configurado em todas as portas dos dois firewalls da topologia. No entanto, o range de IPs disponível foi escolhido sem levar em consideração a quantidade de dispositivos que seriam conectados. Como resultado, sobraram IPs disponíveis, facilitando para que um atacante se conectasse aos switches da topologia e solicitasse um IP via DHCP, obtendo assim livre acesso ao firewall e à rede DMZ. Na Figura 25 mostra como o atacante conseguiu dinamicamente um IP da sub-rede 192.168.2.0/24, através do servidor DHCP.

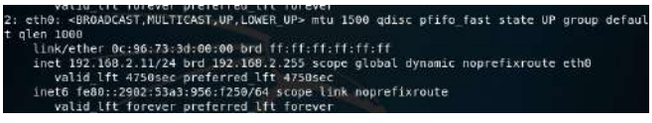


Figura 25: IP do atacante recebido dinamicamente via DHCP

Para evitar que um atacante obtenha um IP via DHCP e tenha acesso não autorizado à rede, deve-se configurar o range de IPs disponíveis no servidor DHCP para corresponder exatamente à quantidade de dispositivos autorizados na rede. Isso reduz a chance de que IPs ociosos sejam usados por atacantes. Além disso, é importante implementar monitoramento e alertas para detectar dispositivos não autorizados na rede.

Essa vulnerabilidade pode resultar em dois tipos de ataques conhecidos: DHCP Starvation Attack e DHCP Flood Attack [20]. No DHCP Starvation Attack, o atacante envia uma grande quantidade de solicitações de novos endereços IPs ao servidor DHCP, esgotando o pool de endereços disponíveis e impedindo que dispositivos legítimos obtenham endereços IP. Já no DHCP Flood Attack, o objetivo é sobrecarregar o servidor DHCP com um grande volume de requisições, causando lentidão ou falhas no serviço.

B. Varredura

Como o atacante conseguiu IP e gateway via DHCP, ele pode usar o Nmap, uma ferramenta de código aberto para exploração de rede e auditoria de segurança, para fazer uma varredura na rede em busca de informações importantes. Sabendo que estava na sub-rede 192.168.0.0/16, ele realizou a varredura em toda a sub-rede, como mostra a Figura 26.

Figura 26: Resultado da varredura na sub-rese 192.168.0.0/16

Algumas informações importantes foram obtidas durante a varredura. Foi descoberto que havia uma máquina com o IP 192.168.1.101 (localizada na DMZ) com a porta 22 aberta, usada para comunicação via SSH. Utilizando a opção -A do Nmap, que permite a detecção do sistema operacional, a verificação de versões, a varredura de scripts e o traceroute, foi possível obter informações detalhadas sobre o host. Descobriu-se que a porta SSH estava executando o serviço OpenSSH e que o sistema operacional era Linux, como mostrado na Figura 27.

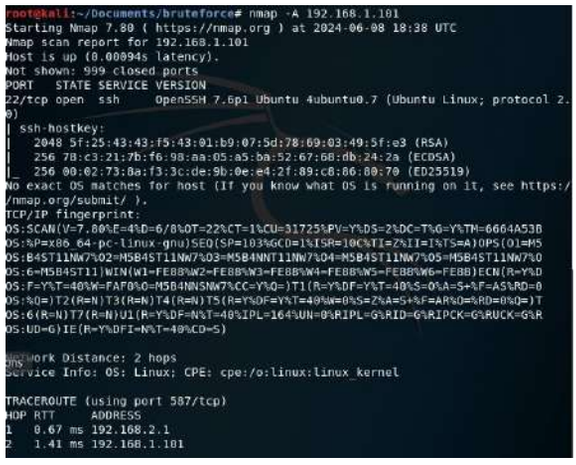


Figura 27: Resultado da varredura no IP 192.168.1.101

C. *Força bruta*

Sabendo que a porta 22 estava aberta e provavelmente executando um servidor SSH, o atacante pode procurar listas de senhas e usuários padrão para tentar um ataque de força bruta, visando obter acesso ao host. A lista de teste utilizada pode ser encontrada em [21].

Um ataque de força bruta é uma técnica de hacking onde o atacante tenta adivinhar senhas ou chaves de criptografia ao tentar todas as combinações possíveis até encontrar a correta. Esse ataque é eficaz contra senhas fracas, mas pode ser demorado e exigir muitos recursos computacionais, principalmente se a senha for complexa ou se houver medidas de segurança, como bloqueio após várias tentativas falhas [22].

Para o ataque de força bruta, foi utilizada a ferramenta Metasploit, um framework de código aberto utilizado para testes de penetração e desenvolvimento de exploits. No ataque, foi configurada uma tentativa de login utilizando a lista de teste com possíveis usuários e senhas no host 192.168.1.101. A configuração do Metasploit pode ser visualizada na Figura 28.

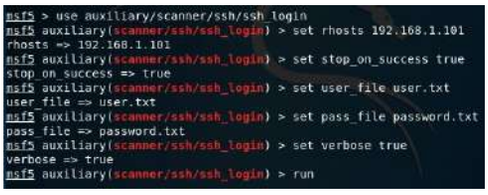


Figura 28: Configuração do Metasploit

Após diversas tentativas sem sucesso, foi descoberto que o usuário do host era "osboxes"e a senha "osboxes.org", como mostra a Figura 29, que são as credenciais padrão das máquinas fornecidas pelo OSBoxes, um serviço que oferece máquinas virtuais pré-configuradas para diversas distribuições de sistemas operacionais.

Figura 29: Resultado da tentativa de força bruta para acesso via ssh

Com o usuário e a senha em mãos, o atacante conseguiu acessar o host utilizando o comando SSH. Isso representa uma grave falha de segurança, pois as credenciais padrão do dispositivo deveriam ter sido alteradas para evitar acessos não autorizados. Manter as credenciais padrão torna o sistema vulnerável a ataques simples e previsíveis. É crucial que, ao configurar novos dispositivos, as senhas e os nomes de usuários padrões sejam substituídos por credenciais fortes e únicas.

Além de ser importante trocar as credenciais padrão, é fundamental implementar autenticação no OpenSSH Server para reforçar a segurança do sistema. A autenticação no OpenSSH Server é um processo que verifica a identidade do usuário antes de conceder acesso ao sistema. Isso é geralmente feito por meio de autenticação baseada em senha, autenticação baseada em chave pública ou uma combinação de ambas.

D. *Man-in-the-Middle (MitM)*

Foi implementado um site HTTP simples na DMZ, contendo um esquema básico de login, conforme ensinado em [18]. No entanto, como o site não utiliza criptografia nem HTTPS, ele é suscetível a ataques cibernéticos.

Com a ferramenta Ettercap do Kali Linux, é possível monitorar uma interface de rede. O Ettercap é uma ferramenta de segurança de rede, utilizada para realizar ataques Man-in-the-Middle (MitM) [23]. Ele permite a interceptação, inspeção e manipulação de tráfego de rede em tempo real, possibilitando a captura de senhas, a injeção de conteúdo malicioso e a realização de ataques de spoofing.

Foi simulado um atacante e uma vítima, localizados na rede interna, na área de 'Server'. Vale ressaltar que o atacante pode se conectar à rede através do servidor DHCP configurado nos Exos.

Para iniciar o ataque, é necessário abrir o Ettercap, selecionar a interface eth0 e escolher a opção Unified Sniffing. A partir desse momento, já é possível visualizar os logs da interface selecionada.

Com o Ettercap, é possível identificar hosts na mesma sub-rede em que o atacante está localizado. Conforme ilustrado na Figura 30, foi possível encontrar os hosts dos Exos e do computador da vítima.

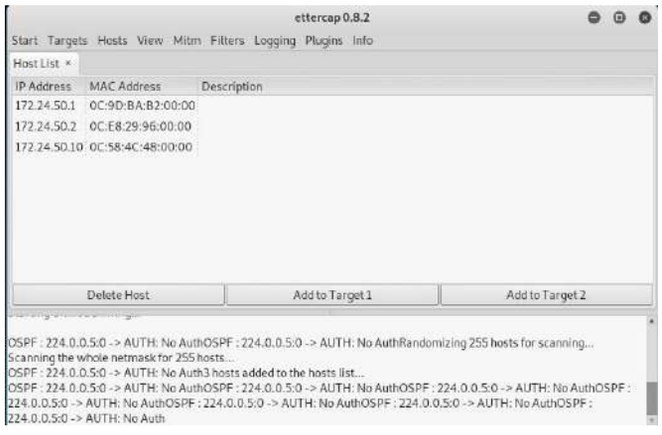


Figura 30: Hosts encontrados no Ettercap

Foi criado um alvo no host 172.24.50.10, que é a vítima, e foi iniciado um ataque MitM do tipo ARP poisoning, conforme mostrado na Figura 31. Esse tipo de ataque funciona manipulando as tabelas ARP da rede, associando o endereço MAC do atacante ao endereço IP da vítima. Dessa forma, o tráfego destinado à vítima é redirecionado para o atacante, permitindo que ele monitore e possivelmente altere os dados transmitidos.

Quando a vítima se conecta ao site exposto na DMZ, que não possui segurança, o atacante consegue visualizar o cabeçalho da requisição, com as credenciais da vítima. Isso é

Figura 31: Ataque de ARP Poisoning no host da vítima

ilustrado nas Figuras 32 e 33. Esta situação é extremamente perigosa, pois permite ao atacante acessar as credenciais da vítima, possibilitando o uso mal-intencionado dessas informações. Tendo em vista isso, o uso de criptografia SSL/TLS é essencial além de manter os certificados digitais válidos e emitidos por uma autoridade certificadora.

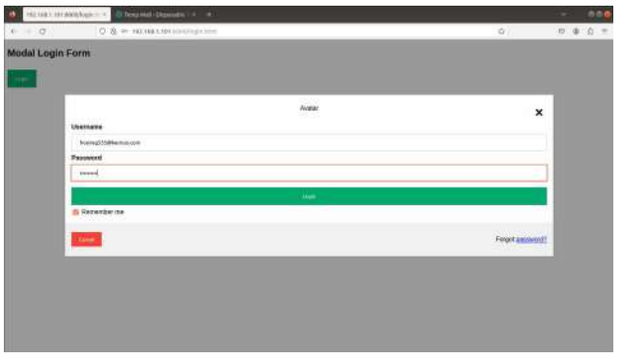


Figura 32: Vítima acessando o site da DMZ

Figura 33: Atacante tendo acesso as credenciais da vítima

E. Clone de Sites

Um ataque bastante conhecido é o de clonagem de sites, onde o atacante cria uma réplica idêntica de um site legítimo para enganar os usuários e roubar suas informações sensíveis [24]. Este ataque pode ser facilmente realizado com a ferramenta Social Engineering Toolkit do Kali Linux. Sabendo que há um serviço HTTP exposto na DMZ, o atacante pode usar essa ferramenta para clonar o site e aplicar técnicas de engenharia social para induzir as vítimas a fornecer suas credenciais e outros dados pessoais.

Isso é realizado utilizando as opções de ataque a websites disponíveis na ferramenta. Conforme ilustrado na Figura 34, com apenas algumas etapas é possível clonar o site da DMZ e hospedá-lo no endereço IP da máquina do atacante. A partir do computador da vítima, o site clonado se apresenta idêntico ao site original da DMZ, como mostrado na Figura 35, induzindo a vítima a acreditar que está acessando o site legítimo e, assim, fornecendo suas credenciais ao atacante.

Para isso, nada melhor do que aumentar a conscientização e o treinamento em segurança. Embora os recursos técnicos possam permitir a autenticação do acesso, os usuários precisam ter um pouco mais de conhecimento digital e procurar sinais de segurança, como o https, representado por um cadeado. entre outras informações cruciais ao navegar na web.

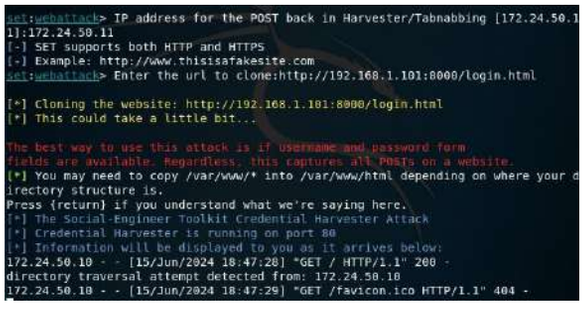


Figura 34: Ferramenta de Engenharia Social

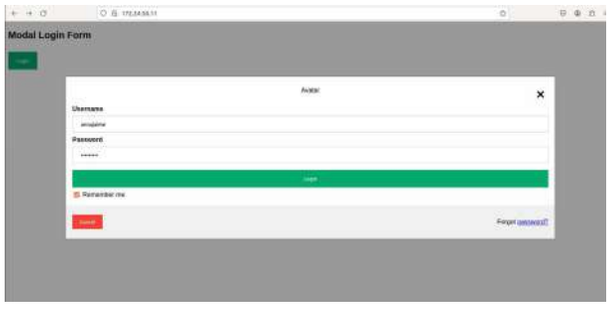


Figura 35: Site clonado pelo atacante

XII. CONCLUSÕES

O objetivo deste projeto é desenvolver e implementar um Network Security Operation Center (NSOC) usando tecnologias e ferramentas sofisticadas como Zabbix, Pfsense, Snort, Vyos, Exos e GNS3. Os resultados mostram a eficácia do NSOC na monitoração e mitigação contínuas de ameaças à segurança cibernética e destacam sua importância estratégica para proteger ativos de rede. As simulações ajudaram a identificar e explorar algumas vulnerabilidades. Isso reforçou a importância de práticas de segurança e políticas de resposta a incidentes.

Para proteger contra novas vulnerabilidades e ataques, recomendamos a continuidade do desenvolvimento de abordagens de segurança adaptativas ao contexto, melhorias nas configurações de segurança dos dispositivos e atualizações regulares dos sistemas.

Por fim este trabalho resume os objetivos, os resultados alcançados e a importância estratégica do NSOC na instituição, visando menos gastos e utilizando em alguns locais, sempre adaptados aos contextos, a implementação desse tipo de segurança.

REFERÊNCIAS

[1] K. Demertzis, N. Tziritas, P. Kikiras, S. L. Sanchez, and L. Iliadis, "The next generation cognitive security operations center: Adaptive analytic lambda architecture for efficient defense against adversarial attacks," *Big Data and Cognitive Computing*, vol. 3, no. 1, 2019. [Online]. Available: https://www.mdpi.com/2504-2289/3/1/6

[2] J. Wang, T. Yan, D. An, Z. Liang, C. Guo, H. Hu, Q. Luo, H. Li, H. Wang, S. Zeng, C. Zhou, L. Ma, and F. Qi, "A comprehensive security operation center based on big data analytics and threat intelligence," *PoS*, vol. ISGC2021, p. 028, 2021.

[3] S. Bhatt, P. Manadhata, and L. Zomlot, "The operational role of security information and event management systems," *Security Privacy, IEEE*, vol. 12, pp. 35–41, 09 2014.

[4] "Zabbix :: The enterprise-class open source network monitoring solution," Jun 2024. [Online]. Available: https://www.zabbix.com/index

[5] A. Pradana, I. R. Widiasari, and R. Efendi, "Implementasi sistem monitoring jaringan menggunakan zabbix berbasis snmp," *AITI*, vol. 19, no. 2, p. 248–262, Nov. 2022. [Online]. Available: https://ejournal.uksw.edu/aiti/article/view/6873

[6] A. Hartono and U. Y. Oktiawati, "Pemantauan router cpe pada jaringan metro ethernet menggunakan zabbix berbasis raspberry pi," *Journal of Internet and Software Engineering*, vol. 2, no. 1, pp. 29–38, Jun. 2021. [Online]. Available: https://jurnal.ugm.ac.id/v3/JISE/article/view/868

[7] "Proxy." [Online]. Available: https://www.zabbix.com/documentation/current/en/manual/api/reference/proxy

[8] "pfsense® - world's most trusted open source firewall." [Online]. Available: https://www.pfsense.org/

[9] K. Patel* and P. Sharma, "A review paper on pfsense – an open source firewall introducing with different capabilities & customization," *International Journal of Advance Research and Innovative Ideas in Education*, vol. 3, pp. 635–641, 2017. [Online]. Available: https://api.semanticscholar.org/CorpusID:169639872

[10] V. Asghari, S. Amiri, and S. Amiri, "Implementing utm based on pfsense platform," in *2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI)*, 2015, pp. 1150–1152.

[11] "Snort," Jun 2024. [Online]. Available: https://www.snort.org

[12] N. Khamphakdee, N. Benjamas, and S. Saiyod, "Improving intrusion detection system based on snort rules for network probe attack detection," in *2014 2nd International Conference on Information and Communication Technology (ICoICT)*, 2014, pp. 69–74.

[13] G. Jain and Anubha, "Application of snort and wireshark in network traffic analysis," *IOP Conference Series: Materials Science and Engineering*, vol. 1119, no. 1, p. 012007, mar 2021. [Online]. Available: https://dx.doi.org/10.1088/1757-899X/1119/1/012007

[14] A. Boyko, V. Varkentin, and T. Polyakova, "Advantages and disadvantages of the data collection's method using snmp," in *2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon)*, 2019, pp. 1–5.

[15] A. H. Alhilali, A. Al Farawn, and A. Y. Mjhool, "Design and implement a real-time network traffic management system using snmp protocol," *Eastern-European Journal of Enterprise Technologies*, vol. 5, no. 9 (125), p. 35–44, Oct. 2023. [Online]. Available: https://journals.uran.ua/eejet/article/view/286528

[16] [Online]. Available: https://www.gns3.com/

[17] MARCONI, Marina de Andrade; LAKATOS, Eva Maria. Fundamentos de metodologia científica. 8ª ed. São Paulo: Atlas, 2017.

[18] "pasan1/simple-fastapi-user-authentication," Jun 2024. [Online]. Available: https://github.com/pasan1/Simple-FastAPI-User-Authentication

[19] "How to create a login form." [Online]. Available: https://www.w3schools.com/howto/howto_css_login_form.asp

[20] A. AbdulGhaffar, S. K. Paul, and A. Matrawy, "An analysis of dhcp vul- nerabilities, attacks, and countermeasures," in *2023 Biennial Symposiumon Communications (BSC)*, 2023, pp. 119–124.

[21] "Seclists - passwords - default-credentials - ssh-betterdefaultpasslist.txt at master · danielmiessler/seclists," Jun 2024. [Online]. Available: https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/ssh-betterdefaultpasslist.txt

[22] "What is a brute force attack? | definition, types how it works," Jun 2024. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/brute-force-attack

[23] "What is a man-in-the middle (mitm) attack? types examples," Jun 2024. [Online]. Available: https://www.fortinet.com/br/resources/cyberglossary/man-in-the-middle-attack.html

[24] Jun 2024. [Online]. Available: https://ironscales.com/guides/ phishing-prevention-best-practices/clone-phishing

COMUNICAÇÕES FONTE DE ALIMENTAÇÃO DE BAIXO CUSTO PARA UTILIZAR EM BANCADA DE MANUTENÇÃO DE RÁDIOS NO EB

Sgt **MICAEL** REBOUÇAS PEREIRA
Sgt **LUCAS GUEDES** DA SILVA

RESUMO

Uma fonte de alimentação de baixo custo é essencial para a manutenção de rádios no Exército Brasileiro (EB), onde a confiabilidade e a eficácia são fundamentais. Em ambientes de bancada, uma solução econômica permite a realização de testes e reparos com eficiência, sem comprometer o orçamento. Para atender às necessidades específicas, a fonte deve fornecer tensões estáveis e ajustáveis, suportar diferentes correntes de consumo e garantir a segurança dos equipamentos e do operador. Além disso, a escolha de componentes acessíveis, mas de qualidade, garante durabilidade e desempenho consistente. A adoção dessa ferramenta na manutenção de rádios militares não só otimiza os recursos disponíveis, como também melhora a prontidão operacional, ao facilitar o trabalho dos técnicos e assegurar que os equipamentos estejam sempre em perfeito funcionamento. Portanto, a implementação de uma fonte de alimentação acessível é uma medida estratégica para o EB.

A ideia de reduzir custos na fonte de alimentação ajuda em sua aquisição em maior quantidade assim como também na aquisição de mais suprimentos para a manutenção dos equipamentos rádios.

Palavras-chave: fonte de alimentação, manutenção, Exército Brasileiro.

1 INTRODUÇÃO

O Brasil enfrentou várias crises financeiras ao longo dos anos que impactaram diretamente as políticas públicas e a alocação de recursos, incluindo cortes significativos no Ministério da Defesa, afetando o Exército Brasileiro.

Nos anos 1980, a crise da dívida externa gerou uma profunda recessão e levou o governo a implementar medidas de austeridade fiscal. O colapso econômico reduziu drasticamente o orçamento militar, resultando em atrasos nos projetos de modernização e na manutenção de equipamentos.

Durante os anos 1990, o Brasil passou por outra fase de dificuldades econômicas, agravada pela hiperinflação e pela necessidade de estabilização econômica. O Plano Real, implementado em 1994, trouxe estabilidade, mas também exigiu cortes nos gastos públicos. O Ministério da Defesa sofreu novamente com orçamentos reduzidos, impactando a capacidade operacional e a prontidão do Exército.

Na década de 2010, o Brasil enfrentou uma recessão severa entre 2014 e 2016, culminando em um ajuste fiscal rigoroso. O Exército foi particularmente afetado, com cortes que reduziram os investimentos em infraestrutura, a compra de novos equipamentos, e até mesmo o custeio de operações básicas.

Essas crises ilustram como as dificuldades econômicas impactam diretamente a capacidade do governo de financiar suas Forças Armadas, obrigando o Exército Brasileiro a operar com recursos limitados e muitas vezes a adiar projetos essenciais para a defesa do país.

O Comando de Comunicações e Guerra Eletrônica do Exército (CCOMGEX), por meio do Centro de Logística (C Log), tem se esforçado para aprimorar a manutenção dos rádios utilizados, especialmente em operações cruciais. Em 2011, foram adquiridas estações de trabalho para realizar a manutenção dos equipamentos de rádio da marca Motorola. No entanto, o alto custo associado a essas estações impediu que cada Organização Militar (OM) recebesse uma estação, e a própria manutenção dessas estações se torna inviável. Com isso, a aquisição de ferramentas de baixo custo torna-se primordial.

2 DESENVOLVIMENTO

> Artigo 57. O procedimento de manutenção tem como propósito estabelecer diretrizes para a condução da manutenção dos variados materiais pertencentes à Classe VII e atualmente em uso no âmbito do Exército. Apesar de ser considerado um processo unitário, na realidade, ele abrange doze diagramas de fluxo distintos, um para cada categoria de equipamento de Comunicações empregado, mesmo que já tenham se tornado obsoletos. (NARMCOMGE, 2019).

De acordo com as orientações da NARMCOMGE, há uma uniformização aplicada ao processo de manutenção para cada categoria que se enquadra o rádio. No contexto dos rádios fabricados pela Motorola e Harris, os quais englobam diversas categorias, o procedimento tendia a se tornar excessivamente complexo para as Organizações Militares portadoras desses Equipamentos. Foi então que em 2022, após o CCOMGEX lançar diversas missões de Manutenção de Rádios em diversas regiões do Brasil, ocorreu uma modificação no artigo 57 da NARMCOMGE, resultando na seguinte redação:

> Art. 57. O processo de manutenção engloba os procedimentos para a Mnt dos MEM Classe VII em uso no Exército, bem como para o trato com os equipamentos obsoletos ou em processo de obsolescência, além da logística reversa do material inservível. (NARMCOMGE, 2022)

Com a manutenção da Classe VII em situação crítica no EB, a Escola de Comunicações estava em busca de soluções para alinhar o processo de manutenção aprendido nos cursos com a realidade das Organizações Militares onde os sargentos qualificados seriam implantados. Foi nesse contexto que, em 2024, o Projeto Interdisciplinar dos alunos do curso Avançado de Eletrônica focou na temática da manutenção de baixo custo dos rádios utilizados pelo Exército, incentivando os futuros especialistas em Eletrônica a encontrar soluções práticas para as demandas existentes.

O projeto, intitulado "FONTE DE ALIMENTAÇÃO DE BAIXO DE CUSTO PARA UTILIZAÇÃO EM BANCADAS DE ELETRÔNICA", foi elaborado pelos alunos: 2º SGT Mnt Com DEIVIDSON FEITOSA DA SILVA, 2º SGT Mnt Com JULES FREITAS FONSECA, 3º SGT Mnt Com ELIAS DA SILVA PEDRO JUNIOR e 3º SGT Mnt Com LUÍS ALENCAR RODRIGUES OLIVEIRA. O foco do trabalho foi apresentar uma alternativa de baixo custo para suprir a necessidade de uma fonte de alimentação de bancada convencional que tem valor no mercado nacional variando entre R$ 1.323,44 e R$ 3.039,90, com valor médio de R$ 2.181,67. O custo associado a essa abordagem equivalia a somente 5,35% do valor médio de mercado, ou seja, R$ 116,86, sendo extremamente acessível para as Organizações Militares do Exército Brasileiro.

Figra 1 – Comparativo de preço de mercado.

Modelo da fonte	Valor Médio
MPL – 1305M	R$ 1.323,44
MPL – 3305M	R$ 3.039,90
Fonte de Baixo Custo	R$ 116,86

Fonte: P.I. - FONTE DE ALIMENTAÇÃO DE BAIXO DE CUSTO PARA UTILIZAÇÃO EM BANCADAS DE ELETRÔNICA

Em contínuo espírito inovador, a seção de Ensino Bravo da Escola de Comunicações, liderada mais uma vez pelo 1º Tenente Adiniz Ferreira, prosseguiu com o enfoque na temática da manutenção no âmbito do Projeto Interdisciplinar do curso Avançado de Eletrônica - 2024. Nessa ocasião, os alunos do curso desenvolveram um passo a passo de como fabricar (montar) uma fonte de alimentação de baixo custo destinada a ajudar

na manutenção dos rádios Motorola e Harris nos diversos escalões da manutenção, com a finalidade de ser adquirido por todas as Organizações Militares que necessitem deste equipamento para ser utilizado por sargentos da Qualificação Militar de Manutenção de Comunicações em seus trabalhos nas bancadas de manutenção eletrônica dos equipamentos rádios, não sendo necessário um curso ou estágio para montar a fonte.

Figra 2 – Fonte de Bancada Variável de Baixo Custo Finalizada.

Fonte: P.I. - FONTE DE ALIMENTAÇÃO DE BAIXO DE CUSTO PARA UTILIZAÇÃO EM BANCADAS DE ELETRÔNICA

3 CONCLUSÃO

O sucesso deste projeto interdisciplinar, dos alunos do curso Avançado de Eletrônica do ano de 2024, não apenas destaca o valor de uma educação prática e inovadora, mas também impulsiona significativamente a eficiência dos processos de manutenção nas forças armadas. Ao equipar os sargentos da Qualificação Militar de Manutenção de Comunicações com ferramentas acessíveis e de fácil implementação, o Exército Brasileiro fortalece sua capacidade de assegurar a prontidão operacional, garantindo a funcionalidade constante dos equipamentos de comunicação, essenciais para o sucesso das missões.

A Escola de Comunicações, ao engajar seus estudantes do curso Avançado de Eletrônica em projetos voltados para soluções de baixo custo, demonstra uma habilidade notável em superar desafios com ideias que são ao mesmo tempo inovadoras, simples e eficazes. A criação da fonte de alimentação de baixo custo reforça o compromisso contínuo dos profissionais de Manutenção de Comunicações em aprimorar os meios necessários para a manutenção dos MEM Classe VII.

Essa convergência de abordagens centradas na prática, inovações educacionais e um foco incisivo na eficiência constrói um ambiente de manutenção mais ágil e eficaz. Como resultado, há um aumento significativo na disponibilidade dos equipamentos vitais para as Organizações Militares, garantindo que as Forças Armadas continuem operando com máxima eficácia, mesmo diante de restrições orçamentárias ou desafios técnicos.

Abstract

A low-cost power supply is essential for maintaining radios in the Brazilian Army (EB), where reliability and efficiency are paramount. In bench environments, an economical solution allows for testing and repairs to be carried out efficiently without straining the budget. To meet specific needs, the power supply must provide stable and adjustable voltages, support different current loads, and ensure the safety of both equipment and operator. Moreover, the choice of accessible yet quality components ensures durability and consistent performance. The adoption of this tool in military radio maintenance not only optimizes available resources but also improves operational readiness by facilitating technicians' work and ensuring that the equipment is always in perfect working order. Therefore, implementing an affordable power supply is a strategic measure for the Brazilian Army.

The idea of reducing costs in the power supply aids in its acquisition in larger quantities as well as in the purchase of more supplies for radio equipment maintenance.

Keywords: ***power supply, maintaining, Brazilian Army.***

4 REFERÊNCIAS

CONTEÚDO, E. **Corte de 44% na verba das Forças Armadas afeta mais a Marinha**. Disponível em:

<https://exame.com/brasil/cortes-no-ministerio-da-defesa-afetam-mais-a-marinha/>. Acesso em: 28 aug. 2024.

FEITOSA, D. S. et al. **FONTE DE ALIMENTAÇÃO DE BAIXO DE CUSTO PARA UTILIZAÇÃO EM BANCADAS DE ELETRÔNICA**. Curso Avançado de Eletrônica. Brasília, 2024.

MURMEL, N. **Brasil corre risco de regredir 40 anos na Defesa, alerta comandante do Exército**. Disponível em: <https://www.defesanet.com.br/defesa/brasil-corre-risco-de-regredir-40-anos-na-defesa-alerta-comandante-do-exercito/>. Acesso em: 28 aug. 2024.

REDAÇÃO. 05 de novembro de 2017. **Exército Brasileiro adquiriu estações de reparo para fazer manutenção em rádios**. Disponível em: https://www.revistamanutencao.com.br/noticias/manutencao/exercito-brasileiro-adquiriu-estacoes-de-reparo-para-fazer-manutencao-em-radios.html. Acesso em: 28 ago. 2024.

COMPUTAÇÃO QUÂNTICA E AS VULNERABILIDADES DOS ATUAIS SISTEMAS CRIPTOGRÁFICOS: RELEVÂNCIA PARA A SEGURANÇA DA INFORMAÇÃO

*SGT DANIEL **BOMFIM** NUNES*
*SGT **DERYCK** MOURA*

RESUMO

A computação quântica, uma tecnologia com potencial para transformar diversos campos da ciência, da tecnologia e consequentemente da sociedade, apresenta elevada relevância para a segurança de dados e informações. A elevada velocidade de processamento e aumento na capacidade de computação das possibilidades gera impactos na performance de diversos setores informacionais, mas também abre portas para violações de segurança. O avanço na implementação da mecânica quântica na base do funcionamento de computadores abre margem para que os alicerces da segurança cibernética, do armazenamento, manipulação e tráfego de dados sejam abalados, principalmente no que tange ao uso da criptografia. Este artigo avalia o impacto potencial da computação quântica sobre os sistemas criptográficos atuais, sua relação com tecnologias fundamentais na sociedade do séc. XXI e aponta algumas estratégias de mitigação para proteger a segurança digital na era da computação quântica.

Palavras-chave: computação quântica, criptografia, algoritmo, segurança da informação.

1 INTRODUÇÃO

A computação quântica surge como uma revolução científica e tecnológica com o potencial de transformar diversas áreas, especialmente a criptografia. Em 1994, o matemático Peter Shor apresentou um algoritmo que demonstrou como os computadores quânticos poderiam resolver problemas matemáticos complexos de forma exponencialmente mais rápida do que os computadores tradicionais. Essa descoberta revelou uma ameaça iminente aos sistemas de segurança que utilizam criptografia baseada na dificuldade de fatoração de números primos. Os sistemas criptográficos atuais, como o RSA, são amplamente utilizados para proteger informações sensíveis, confiando na dificuldade de fatorar grandes números como uma barreira intransponível para potenciais invasores. No entanto, a capacidade teórica dos computadores quânticos de quebrar esses códigos em um tempo razoável coloca em risco a segurança dos dados protegidos por essas técnicas.

Essa ameaça enfatiza a necessidade urgente de desenvolver novas formas de criptografia que possam resistir aos ataques quânticos. À medida que a computação quântica avança, a transição para algoritmos criptográficos quânticos seguros torna-se uma prioridade para garantir a proteção das informações na era pós-quântica.

2 DESENVOLVIMENTO

A exploração das propriedades da mecânica quântica, como o entrelaçamento, a interferência e a superposição de estados para realizar operações computacionais de forma mais eficiente permitiu o desenvolvimento do que se conhece por computação quântica. Em vez de bits, que são a unidade básica informacional dos computadores clássicos, os computadores quânticos utilizam qubits, que podem existir simultaneamente em múltiplos estados graças à superposição quântica. O entrelaçamento quântico também permite que qubits estejam interligados, de modo que o estado de um qubit influencia o estado de outro, mesmo que estejam separados por grandes distâncias. Essas propriedades únicas possibilitam o processamento massivo de informações simultaneamente, revolucionando a capacidade de cálculo.

Em comparação com os computadores clássicos, que processam informações de forma sequencial utilizando bits em estados de 0 ou 1, os computadores quânticos oferecem uma capacidade de processamento exponencialmente superior para certos tipos de problemas. Isso se deve ao fato de que os qubits podem representar e manipular várias

possibilidades ao mesmo tempo. Por exemplo, enquanto um computador clássico precisaria testar cada solução possível para um problema, um computador quântico pode explorar todas as soluções paralelamente, acelerando drasticamente o processo de cálculo.

Essa capacidade permite que um computador quântico execute certos algoritmos, como o de Shor, muito mais rapidamente do que qualquer computador clássico. O poder de processamento superior da computação quântica abre novas possibilidades em áreas como criptografia, simulação de sistemas físicos complexos e otimização. No entanto, também apresenta desafios únicos, como a manutenção da coerência quântica e a correção de erros quânticos, que precisam ser superados para a plena realização dessa tecnologia.

Ao citarmos a supremacia dos computadores quânticos frente aos computadores clássicos e os respectivos algoritmos de criptografia usados, é natural surgir o questionamento sobre quais fraquezas evidenciam estes problemas. No campo da criptografia assimétrica, a qual faz uso de duas chaves, uma pública e outra privada, um algoritmo amplamente utilizado é o Rivest-Shamor-Adleman (RSA). A segurança da chave criptográfica utilizada reside na dificuldade matemática da fatoração de números primos muito grandes (chaves que variam de 512 até 8192 bits). Tal entrava se dá pelo fato de que mesmo os computadores com capacidade de processamento mais robusta demorariam milhões de anos para quebrar tais chaves pelos métodos de fatoração existentes. Se levaria mais tempo do que a própria existência da humanidade para quebrar as chaves criptográficas usada no protocolo RSA, então qual a fraqueza existente? A vulnerabilidade, atualmente, não é diante dos computadores clássicos, mas sim dos eventuais computadores quânticos, pois estes fazem uso da superposição de estados para elevar exponencialmente a velocidade de processamento simultâneo de dados. Isto permite que uma tarefa que levaria milhões de anos ocorra em horas, minutos ou até mesmo segundos.

A utilização do algoritmo de Shor para exploração de vulnerabilidades dos sistemas criptográficos atuais, é um exemplo de metodologia que pode decifrar as chaves utilizadas pelo RSA, por exemplo. Para que esta aplicação logre êxito é fundamental compreender que o uso de computadores quânticos é essencial, pois a utilização do algoritmo para fatorar números primos aliada ao incremento exponencial no cômputo das probabilidades dos valores fornecidos pela superposição dos estados faz com que o tempo de cálculos dos fatores que geraram a chave mudem de um tempo exponencial para um tempo polinomial, o que significa uma robusta redução no tempo de quebra da chave.

É possível imaginar um cenário após o desenvolvimento de um computador quântico que implemente o algoritmo de Shor para fatorar números maiores que 2048 bits. Este panorama parece ser um tanto caótico, pois diversas informações confidenciais trafegadas nas redes poderiam ser violadas. Diante disto, é necessário pensar sobre como garantir a segurança dos diversos setores que fazem uso da criptografia. Os pesquisadores Charles Henry Bennett e Gilles Brassard desenvolveram, em 1984, um protocolo conhecido como BB84. A ideia era propor um sistema de distribuição de chaves baseado em alguns princípios da mecânica quântica. De modo simplificado podemos entender que a impossibilidade de medir a informação de uma partícula sem alterar seu estado e o princípio da não-clonagem impedem que os dados trafegados sejam interceptados sem detecção. Deste modo, a chave estabelecida seria segura. Certamente um atacante pode buscar acessar as máquinas envolvidas na transação para copiar a chave após ser armazenada. Depois disso ele tentaria quebrar essa sequência de bits. O detalhe é que a própria geração dos bits da chave segue um processo aleatório para o qual, em princípio, não há uma fórmula específica para reverter o processo e encontrar o valor original. Além disso, existem pesquisas de algoritmos pós-quânticos, os quais pretender ser implementados em computadores clássicos por meio de novas funções e metodologias matemáticas que proponham problemas diferentes da fatoração de números primos. O ponto crucial é elaborar um problema para o qual a complexidade seja tal que mesmo um

computador quântico não conseguiria resolvê-lo em tempo humanamente válido.

3 CONCLUSÃO

As tecnologias digitais utilizam algoritmos criptográficos em diversos setores da sociedade. Há implementações no tráfego de informações em serviços de saúde, ensino, transações financeiras por meio do protocolo HTTPS, por exemplo, o qual usa criptografia assimétrica em sua base. Este ponto, por si só, já se torna crítico pelo volume e relevância das informações pessoais compartilhados. Sistemas como criptomoedas, assinaturas digitais, acesso a servidores dentre outros para os quais a criptografia é essencial. Assim, é premente compreender que a inevitabilidade dos perigos que a computação quântica pode trazer para a segurança da informação, seja de um computador pessoal ou de uma nação, é uma realidade. Para lidar com esta realidade cada vez mais próxima é necessário investir em pesquisa, educação científica, integração entre instituições de pesquisa do Estado e empresas para pensar e desenvolver soluções no setor de tecnologias quânticas, principalmente no que concerne à criptografia quântica.

Abstract

Quantum computing, a technology with the potential to transform various fields of science, technology, and consequently society, presents significant relevance for data and information security. The high processing speed and increased computational capacity generate impacts on the performance of various informational sectors, but also open doors for security breaches. The advancement in the implementation of quantum mechanics as the foundation of computer operation raises concerns that the pillars of cybersecurity, data storage, manipulation, and traffic, could be compromised, especially in terms of cryptography. This article assesses the potential impact of quantum computing on current cryptographic systems, its relationship with fundamental technologies in 21st-century society, and suggests some mitigation strategies to protect digital security in the era of quantum computing.

Keywords: ***Quantum computing, cryptography, algorithm, information security***

4 REFERÊNCIAS

CARVALHOSA, Jonathan Correia - Aplicação de Reticulados em Criptografia. Rio de Janeiro: IME, 2012.

FREITAS, Adriana Xavier – Algoritmo de Shor e sua aplicação à fatoração de números inteiros. S.I.: UFMG, 2010.

GALVÃO, Ernesto F. O que é Computação Quântica. Vieira e Lent, 1o edição, 2007

LOPES, Bianca de Meira; LIMA, Thainá Lucciola Hipolito de. Fatoração de números com recursos da computação quântica. Projeto de Final de Curso – Instituto Militar de Engenharia, Rio de Janeiro, 2022.

OLIVEIRA, Ivan S.; SARTHOUR, Roberto S. Computação Quântica e Informação Quântica. Rio de Janeiro: CBPF, 2004.

AS COMUNICAÇÕES MILITARES NA MONTANHA UMA ANÁLISE DOS MEIOS DE COMUNICAÇÕES EMPREGADOS NO AMBIENTE OPERACIONAL DE MONTANHA

Sgt **Matheus Henrique** de Souza

RESUMO

O ambiente operacional de montanha, em virtude do terreno escarpado e compartimentado, apresenta inúmeras dificuldades às operações, especialmente no que diz respeito à manutenção do comando e controle. Nesse contexto, o tema do presente artigo é o emprego dos meios de comunicações pelos Batalhões de Infantaria Leve de Montanha do Exército Brasileiro nesse ambiente inóspito para as comunicações militares. Para atingir as conclusões apresentadas no presente artigo de opinião, as experiências pessoais deste autor foram qualificadas com a Doutrina Militar Terrestre mais atual, materializada em cadernos de instrução e em artigos científicos. Com isso, foi possível identificar os sistemas de comunicações nos quais esses batalhões se inserem e as frações responsáveis pela operação desses meios. Ademais, foi possível categorizar esses meios em rádio, satelitais e fio, a fim de estabelecer vantagens e desvantagens no seu uso relacionadas ao ambiente operacional em questão.

Palavras-chave: comunicações, rádio, satelital, meio fio, ambiente operacional de montanha.

1. INTRODUÇÃO

No ambiente operacional de montanha, são enfáticas as dificuldades em estabelecer enlaces de comunicações no emprego do rádio. Esses desafios aumentam quando as frações nas quais o enlace é pretendido demandam grande flexibilidade em seus deslocamentos. Por isso, ao passo em que o rádio é o meio de comunicação mais desejável, por ser muito flexível, as dificuldades no seu uso trazem óbices notórios às operações em montanha - para além das preocupações com a segurança. Por esse motivo, cresce de importância debater técnicas, táticas, procedimentos e estratégias de emprego dos meios de comunicações militares em geral.

Partindo dessas premissas, o presente artigo analisa as possibilidades e as limitações dos principais meios de comunicações atualmente empregados nos Batalhões de Infantaria Leve de Montanha (BIL Mth). Essas Organizações Militares (OM) são as menores frações do Exército Brasileiro em que se pode analisar os sistemas de comunicações utilizados nas operações de montanha propriamente ditas – já que a 4ª Companhia de Comunicações Leve de Montanha (4ª Cia Com L Mth) instala o sistema da brigada.

O primeiro tópico do desenvolvimento apresenta a segmentação de funções e a responsabilidade pelas ligações no âmbito dos BIL Mth. Os tópicos seguintes adentram no objetivo propriamente dito deste estudo, que é analisar os principais sistemas de comunicações estabelecidos por essa unidade tipo e os meios de comunicações utilizados.

Ao fim, foi possível categorizar os meios de comunicações empregados, conforme a doutrina militar clássica, em: rádio, satelital e fio. As particularidades dessas categorias foram pormenorizadas nas vantagens e desvantagens dos equipamentos atualmente empregados nos BIL Mth da 4ª Brigada de Infantaria Leve de Montanha (4ª Bda Inf L Mth ou Bda Mth). Com esse enfoque foi possível destacar a predileção na Bda Mth pelo uso dos equipamentos Motorola e a preterição do meio fio, em favor do rádio e dos equipamentos satelitais.

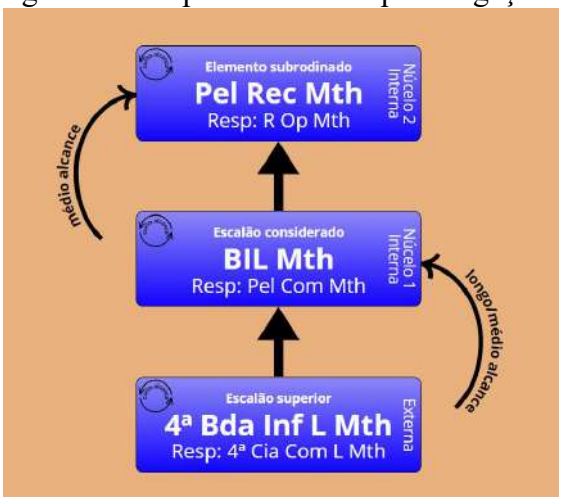
2. DESENVOLVIMENTO

2.1 AS COMUNICAÇÕES NOS BIL MTH

Na atribuição das responsabilidades pelas ligações, prevalece a lógica de que o estabelecimento do Sistema de Comunicações da Operação é dever do escalão imediatamente superior; cabendo ao escalão inferior se adequar a esse sistema (Brasil, 2018, p. 4-2). Com base nisso, é possível dividir as tarefas de Comunicações dos BIL Mth em dois núcleos: o Pelotão de Comunicações dos BIL Mth (Pel Com Mth), que se

adequa ao Sistema de Comunicações desenvolvido pela 4ª Bda Inf L Mth (longo/médio alcance); e estabelece o Sistema de Comunicações entre o Cmdo do Btl e as frações descentralizadas (médio alcance). O segundo núcleo são os Rádio Operadores das frações que operam descentralizadas em montanha (R Op Mth), com as atribuições de se adequar ao sistema estabelecido pelo Pel Com Mth e estabelecer as comunicações internas da fração (curto alcance).

Figura 1 – Responsabilidades pelas ligações.



Fonte: do autor, 2024.

Sendo assim, o Pel Com Mth tem a missão de instalar, explorar e manter, com oportunidade e eficiência, os sistemas fio, rádio e mensageiros do BIL Mth (Brasil, 2022[i], p. 2-69 e 2-83). Dessa forma, por meio da construção de um C Com no Posto de Comando Principal (PCP) e no Posto de Comando Tático (PCT) - se houver -, esse pelotão viabiliza o contato entre o Cmdo do Btl e as tropas desdobradas no terreno (inclusive o Pelotão de Reconhecimento dos BIL Mth - Pel Rec Mth).

O Pel Com Mth também se adequa ao Sistema de Comunicações da Bda Mth (nesse caso, provido pela 4ª Cia Com L Mth). Ainda supre com meios os R Op Mth, de forma que eles possam estabelecer as comunicações nas suas frações. Com isso posto, passa-se à análise dos meios utilizados nas ligações internas dos BIL Mth.

2.2 OS RÁDIOS NA MONTANHA

O rádio é o principal meio de Comunicações utilizado no nível brigada (Brasil, 1998, p. 4-7), o que também ocorre na Bda Mth. Isso se dá em virtude da alta flexibilidade desse meio, que normalmente opera sem a necessidade de instalações físicas mais duradouras, permitindo vencer com maior facilidade os obstáculos do terreno compartimentado.

No âmbito dos BIL Mth se emprega o rádio MPR-9600, Falcon II, da Harris, que opera na faixa de frequência HF, conforme relata Pestana (2019, p. 21). Embora o seu uso se dê mediante empréstimo de outras OM não pertencentes à Bda Mth, esse rádio tem sido a muito utilizado para o estabelecimento das ligações com os Centros de Comunicações (C Com) dos Btl, assim como recomenda a DMT, nos seguintes termos:

> Considerando as amplas frentes ocupadas e a distância entre os comandos envolvidos, cresce de importância a utilização de equipamentos que operem em HF, mesmo nos escalões menores, ou de postos de retransmissão. (Brasil[1], 2020, p. 5-6)

A DMT também recomenda o uso de estações repetidoras em terreno montanhoso, desde que sejam dotadas de grande mobilidade (Brasil[1], 2020, p. 5-1). Podem ser usados com essa finalidade tanto as GTR8000 da Motorola, quanto o próprio rádio Harris 7800V-HH configurado como um repetidor de voz em rede, utilizando a forma de onda *TDMA networking waveform* (TNW). Todavia, não há registros de uso do rádio 7800V-HH como repetidor de voz nas operações em montanha, sendo empregada normalmente a estação repetidora GTR8000.

Os equipamentos repetidores normalmente são instalados em localizações de altitude destacada no terreno. Com o uso adicional de sistemas de predição de enlace, o emprego de estações repetidoras permite a mitigação das zonas de silêncio. A elevada altitude da instalação ainda aumenta a distância do enlace, já que a área na qual os rádios conseguem estabelecer visada direta com as antenas da repetidora é maior do que a área em que a visada direta entre os rádios é possível. É o que se pode perceber na Fig. 2, em que um sistema

de predição de enlace foi utilizado para buscar o melhor ganho potencial de alcance no uso da repetidora GTR8000 na Serra de São José, em São João del-Rei-MG.

Figura 2 – sistema de predição de enlace da repetidora GTR8000 em montanha.

Fonte: Ribeiro, Souza, Martinbianco, Varandas, 2023, p. 138.

A escolha entre essas alternativas para a comunicação entre o C Com dos Btl e as frações isoladas vai depender do contexto operacional em que essas frações atuam. O rádio HF é mais adequado para uma tropa em deslocamento, principalmente por ocasião das infiltrações em território inimigo. Essa conclusão decorre da constatação de que o rádio HF são menos robustos, tendo instalação e operação mais simplificadas que as repetidoras GTR 8000. Por isso, a instalação da repetidora é mais recomendada nas posições em linhas amigas, especialmente porque limita muito a mobilidade das unidades que a operam.

Figura 3 – componentes da repetidora GTR8000 distribuídos no fardo de combate.

Fonte: arquivo pessoal de militar da 4ª Cia Com L Mth.

Para diminuir as dificuldades de mobilidade no emprego da GTR8000, militares da 4ª Cia Com L Mth estão desenvolvendo pesquisa que visa adaptar essa repetidora, de forma que seu peso seja significativamente reduzido e possa ser transportada no fardo de combate (mochila de grande capacidade) – Fig. 3.

Independentemente de qual seja a escolha para a ligação entre o C Com e o Pel Rec Mth, o fato é que as OM da 4ª Bda Inf L Mth dispõem, majoritariamente, de equipamentos rádio da empresa Motorola, motivo pelo qual têm preferido utilizá-los, em detrimento dos rádios da empresa Harris – cuja disponibilidade é muito escassa (Silva, p. 68, 2021).

2.3 OS EQUIPAMENTOS SATELITAIS NA MONTANHA

Os equipamentos satelitais utilizados atualmente na Bda Mth são: o *Broadband Global Area Network* (BGAN), os telefones satelitais e os *SPOT* (Brasil, 2022[2], p. 5-2 a 5-4). Eles garantem o enlace de dados e a consciência situacional entre o Cmdo dos BIL Mth e as frações descentralizadas. Os rádios HF ou os rádios da Motorola utilizados em conjunto com a GTR80000, apesar de serem capazes de transmitir dados, são empregados somente como enlace de voz, porque a transmissão de dados por esses meios reduz significativamente o alcance, o que normalmente inviabiliza a sua utilização nas operações em montanha.

A utilização dos equipamentos de comunicações satelitais citados, em detrimento do emprego do Sistema de Comunicações Militares por Satélite (SISCOMIS), é de fato o que melhor se adequa às necessidades dos BIL Mth. O BGAN e os telefones satelitais garantem grande mobilidade para o Pel Rec Mth e permitem um enlace de dados satisfatório (internet e EBnet); além de manter a consciência situacional, porque possibilitam o compartilhamento de posição geográfica quando atrelados ao uso do SPOT (Brasil, 2022[2], p. 5-3). O uso do SISCOMIS nas Op Mth tem o óbice da mobilidade restringida pela robustez (Fig. 4), além da maior dificuldade no alinhamento da sua antena, bem como a necessidade de uma fonte de energia mais robusta – enquanto os outros aparelhos dependem apenas de uma pequena bateria de energia a eles atrelada.

Figura 4 – militar operando o SISCOMIS durante

Fonte: redes sociais da 4ª Cia Com L Mth, 2023.

Apesar disso, é importante ressaltar que os equipamentos satelitais utilizados atualmente possuem dois fatores negativos muito significativos, quando comparados ao SISCOMIS. O primeiro é que o BGAN, o SPOT e os telefones satelitais exigem, além dos custos de aquisição, a alocação significativa de recursos para adição de créditos sempre que são utilizados. Já os gastos do SISCOMIS se resumem aos custos de aquisição, uma vez que até a sua manutenção é realizada no Centro de Comunicações e Guerra Eletrônica do Exército (CCOMGEX).

O outro fator negativo diz respeito ao gestor dos satélites utilizados. Isso porque os outros equipamentos utilizam satélites estrangeiros para seu funcionamento, o SISCOMIS utiliza o Satélite Geoestacionário de Defesa e Comunicações Estratégicas, que é gerido pelo Ministério da Defesa. Isso faz com que a utilização do SISCOMIS se mostre muito mais segura em eventual conflito armado, haja vista não depender de relações diplomáticas favoráveis.

2.4 O MEIO FIO NA MONTANHA

Além dos rádios, o Pel Com Mth também deve estar apto a empregar os meios de comunicações por fio. Sobre o emprego desse meio, o CI Emprego do Guia de Montanha esclarece que:

> A comunicação com fio é um meio muito seguro e pode ser usado com grandes vantagens em áreas montanhosas, principalmente em Op Def [...] Devido à pequena confiabilidade das comunicações rádio, é importante que o sistema com fio funcione continuamente, tanto nos deslocamentos como nas situações estáticas. (Brasil, 2022[2], p. 5-5)

Apesar da previsão doutrinária, o ambiente de montanha apresenta uma vasta quantidade de situações que podem prejudicar a comunicação por fio (Brasil, 2020, p. 6-7 e 6-8), além de representar significativa restrição à locomoção da tropa. Por isso e por não permitir transmissão de dados, o fio duplo telefônico (FDT) é pouco empregado nos adestramentos em montanha. Seu uso é restrito às instalações do PCP da Bda para estabelecer uma ligação telefônica entre o C Com Bda e o posto rádio a ele vinculado.

Por outro lado, a ligação principal entre o C Com e seu posto rádio depende atualmente de um enlace de dados. Para isso podem ser usadas antenas PTP (*point-to-point*) da Motorola, cabos de par trançado ou cabos de fibra ótica. Porém o uso de cabos de dados restringido severamente a distância entre as instalações.

No âmbito dos BIL Mth o emprego do FDT é ainda mais raro, porque as frações demandam grande mobilidade no Teatro de Operações. Sendo assim, o enlace de dados principal no nível dos BIL Mth é feito com o meio satelital, preterindo até mesmo o cabeamento de dados.

3. CONCLUSÃO

O ambiente operacional de montanha demanda o emprego de técnicas, táticas e procedimentos de Comunicações específicos para superar as dificuldades impostas pela alta compartimentação do terreno e pela atuação descentralizada das frações. Nesse contexto, cresce de importância a utilização dos meios rádios e satelitais, que garantem maior mobilidade à tropa. Os equipamentos satelitais ganham especial importância, posto que são o principal *link* de dados entre as frações e o Cmdo do Btl.

Quanto aos equipamentos empregados, as OM da Bda Mth dispõem majoritariamente de rádios Motorola, motivo pelo qual têm optado por utilizá-los – o que não descarta o uso de equipamentos Harris, principalmente o rádio HF. Nesse contexto, o uso de estações repetidoras GTR8000 é mais favorecido, buscando enlaces de média e longa distâncias. Porém, o uso dessa repetidora é mais adequado nas linhas amigas, por restringir severamente a mobilidade da tropa.

ABSTRACT

The mountain operational environment, due to the steep and compartmentalized terrain, presents numerous difficulties to operations, especially regarding to maintaining command and control. In this context, the theme of this article is the use of communications means by the Brazilian Army's Mountain Light Infantry Battalions in this inhospitable environment for military communications. To reach the conclusions presented in this opinion article, this author's personal experiences were qualified with the most current Land Military Doctrine, materialized in instruction notebooks and scientific articles. With this, it was possible to identify the communications systems in which these battalions are inserted and the fractions responsible for the operation of these means. Furthermore, it was possible to categorize these means into radio, satellite and wire, in order to establish advantages and disadvantages in their use related to the operational environment in question.

Keywords*: communications, radio, satellite, wire, mountain operational environment.*

4. REFERÊNCIAS

AQUINO, Lucas; DE SOUZA, Matheus Henrique; MARTINBIANCO, Breno; RIBEIRO, Pedro Felippe de Lima; VARANDAS, William Ferreira de Paula. O emprego da repetidora Motorola GTR 8000 no ambiente operacional de montanha. **O Adjunto**, Cruz Alta, vol. 11, n. 01, 2023. Disponível em: https://www.ebrevistas.eb.mil.br/adj/article/view/12444/9950. Acesso em: 9 ago. 2024.

BRASIL. **As Comunicações na Brigada**. Manual de Campanha C 11-30. 2ª ed. Brasília, DF: Estado-maior do Exército, 1998.

BRASIL. **As Comunicações na Força Terrestre**. EB70-MC-10.241. 1ª ed. Brasília, DF: Comando de Operações Terrestres, 2018.

BRASIL. **Adestramento básico das unidades de infantaria de montanha**. EB70-PP-11.275. Edição Experimental. Brasília, DF: Comando de Operações Terrestres, 2022[i].

BRASIL. **Emprego do Guia de Montanha**. EB70-CI-11.468. 1ª ed. Brasília, DF: Comando de Operações Terrestres, 2022[ii].

BRASIL. **O Pelotão de Reconhecimento do Batalhão de Infantaria Leve de Montanha.** EB70-CI-11.435. Edição Experimental. Brasília, DF: Comando de Operações Terrestres, 2020.

PESTANA, Marcello de Almeida Ribeiro. **Possibilidades e limitações do pelotão de reconhecimento de montanha no monitoramento**

de RIPI em apoio a uma brigada em operações defensivas. Trabalho de Conclusão de Curso apresentado requisito parcial para a obtenção do grau de Aperfeiçoamento em Operações Militares. Rio de Janeiro: Escola de Aperfeiçoamento de Oficiais, 2019. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/5306/1/Artigo%20-%20Cap%20Marcello%20Ribeiro.pdf. Acesso em: 17 jan. 2023.

SILVA, Thiago Tadeu de Resende. **Possibilidades da 4ª Brigada de Infantaria Leve de Montanha para atuação no combate moderno**. Projeto de pesquisa apresentado como pré-requisito para a matrícula no Programa de Pós-graduação *lato sensu* em Ciências Militares, com ênfase em Defesa. Rio de Janeiro: Escola de Comando e Estado-Maior do Exército - Escola Marechal Castello Branco, 2021. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/10123/1/MO%206485%20-%20THIAGO%20TADEU%20de%20Resende%20Silva.pdf. Acesso em: 17 jan. 2023.