MAIA: Methodology for Assessing the Impacts of Threats to Information Systems

Albany Neto*
Fátima Duarte-Figueiredo*
albanybarbosa2@gmail.com
fatima.duartefigueiredo@gmail.com
Pontifícia Universidade Católica de Minas Gerais (PUC Minas)
Belo Horizonte, MG, Brasil

Abstract

Context: Cyberattacks have increased in the last decades. The lack of security results in scenarios full of vulnerabilities in information systems. A pentest can be defined as a proactive attempt to assess the security of an information system. It is mandatory in specific organizational scenarios and must be performed by third-party companies, which can imply high costs for the organization.

Problem: Some organizations are often unfamiliar with a pentest or cannot pay for it. Other solutions must be proposed for them.

Solution: An Information System Threat Impact Assessment Methodology (MAIA) easy to follow was this work's objective. The goals were the methodology itself and the index that could quantify the vulnerabilities' impacts.

IS Theory: This work followed the General Systems Theory, in particular with regard to systems security.

Method: The research is prescriptive in nature, and its evaluation was carried out through a case study in a big company. The results are both quantitative and qualitative.

Summary of Results: The practical results in a real organization show the vulnerabilities identified, and the final vulnerability index indicated a high risk to the company. It shows the MAIA applicability.

Contributions and Impact on the IS area: The main contribution is a methodology that is an alternative approach to traditional pentests. The methodology may be conducted by multidisciplinary teams. Decisions regarding the correction of vulnerabilities can be taken based on the results of MAIA.

Keywords

Information Systems Security, Penetration Testing, Attack, Threats, Vulnerabilities, Methodology, Quantification, Risks

1 Introdução

O crescente valor atribuído a dados faz com que sejam frequentemente referidos como o novo petróleo mundial. Com isso, os ataques cibernéticos têm aumentado em quantidade e complexidade, como descrito em [22]. Considerando o mundo atual de sistemas de informação conectados a cidades inteligentes, Internet das Coisas e de veículos, os riscos aumentam ainda mais [35].

O problema de pesquisa é a constante exposição de sistemas de informação de organizações diversas a ameaças cibernéticas. O mundo está cada vez mais conectado, as redes 5G e 6G trazem a ideia de micro operadores[9], o que causa mais descentralização e pulverização de sistemas na Internet. A defasagem na segurança digital, somada à existência de dados valiosos, resulta em cenários repletos de vulnerabilidades no domínio de aplicações organizacionais. Como exemplos de exploração de vulnerabilidades, podem ser citados vazamentos de e-mails e de senhas, exposições de *logs*, controladores [10], arquivos, códigos e dados abertos indevidamente. Quando vulnerabilidades são exploradas por criminosos, há prejuízos funcionais e financeiros, como mostram os autores de [2] e [18].

A motivação do trabalho se refere às abordagens proativas de defesa, como os testes de invasão, também conhecidos como *pentests*, para as ameaças cibernéticas . Um *pentest* pode ser definido como uma tentativa proativa e autorizada de avaliar a segurança de uma infraestrutura de TI (Tecnologia da Informação). Um *pentest* explora vulnerabilidades em redes e sistemas, conforme dizem os autores de [31] e [7].

Embora seja uma prática essencial, principalmente em cenários que exigem conformidade com regulamentações de segurança, sua execução geralmente demanda equipes especializadas e serviços terceirizados, o que pode representar um custo elevado para organizações menores. Muitas empresas de pequeno porte desconhecem essas práticas ou não possuem orçamento suficiente para contratá-las.

O objetivo geral deste trabalho foi o desenvolvimento de uma metodologia de avaliação de impactos de ameaças a sistemas de informação (MAIA), fácil de ser conduzida por equipes internas de uma organização, não demandando contratações de terceiros. A metodologia MAIA visa à identificação de ameaças ou vulnerabilidades em sistemas de informação. Ela é baseada em conceitos similares aos de *pentests* tradicionais e objetiva desmistificar testes de invasão e tornar corriqueira a busca por vulnerabilidades dos sistemas. Como objetivos específicos, quatro fases de MAIA foram detalhadamente especificadas: coleta de informações, enumeração, exploração e análise de exposição de vulnerabilidade.

A originalidade científica está relacionada à quarta fase que difere MAIA das demais metodologias da literatura. Ela inclui os cálculos de índices de exposição das vulnerabilidades (IEV) encontradas nas fases anteriores e, também, o cálculo de um índice geral de exposição a vulnerabilidades ($IEVg$), que indica o grau de exposição que a empresa corre e o quão urgentes são as tomadas de decisão para mitigar os riscos. Os índices calculados englobam níveis de severidade da vulnerabilidade, potencial de exploração pela vulnerabilidade encontrada, impacto de um ataque, se bem-sucedido, existência de mitigação disponível e probabilidade de ocorrência de ataque. MAIA

*Both authors contributed equally to this research.

oferece flexibilidade em termos de fases e adaptabilidade às necessidades da organização. MAIA é baseada em estratégias similares às de um *pentest*, ela mapeia e identifica falhas de segurança.

A contribuição deste artigo é a descrição e a exemplificação de uso de uma metodologia diferente dos *pentests* tradicionais. Além de introduzir a quantificação de vulnerabilidades que permite a avaliação de impactos de ameaças que possam ser causadas por vulnerabilidades do sistema, MAIA é fácil de ser seguida e pode ser executada por equipes internas, sem custos adicionais à organização, o que justifica a sua adoção. Um estudo de caso é apresentado para ilustrar a aplicação da MAIA. Este trabalho pode ser relevante para organizações que não adotam medidas de identificação de vulnerabilidades em seus sistemas de informação. Seguindo as quatro fases de MAIA, as equipes podem se surpreender com os índices de ameaças em vulnerabilidades expostas.

O restante do artigo está organizado da seguinte maneira: a Seção 2 apresenta o Referencial Teórico e os Trabalhos Relacionados, a Seção 3 descreve a metodologia MAIA, na Seção 4, o estudo de caso e seus resultados são apresentados e a Seção 5 conclui e apresenta trabalhos futuros.

2 Referencial Teórico e Trabalhos Relacionados

Esta seção apresenta os principais conceitos e os trabalhos da literatura relacionados ao tema.

2.1 Segurança da Informação: Conceitos fundamentais

A segurança dos sistemas de informação visa confidencialidade, integridade e disponibilidade dos mesmos. Seus pilares fornecem a base para mitigar ameaças, garantindo legalidade, autenticidade e privacidade [27].

De acordo com um estudo de Erkan-Barlow [14], os ataques cibernéticos têm aumentado significativamente, afetando organizações de diversos setores. A pesquisa destaca que os ataques impactam negativamente a lucratividade das empresas, especialmente nos períodos seguintes à violação. Organizações maiores e privadas tendem a sofrer mais do que as menores e públicas, com consequências como a redução de receitas, aumento de custos e diminuição da confiança dos clientes.

Para garantir qualidade de serviço em sistemas de informação, alguns requisitos não-funcionais devem ser traduzidos em parâmetros de desempenho e segurança [16]. Este trabalho apresenta uma metodologia que aborda a segurança dos sistemas de informação. A tríade de ameaças, vulnerabilidades e ataques é central no domínio de segurança da informação. Ameaça refere-se a qualquer evento ou entidade que possa causar danos aos dados e aos sistemas[11]. Vulnerabilidade é uma falha ou deficiência em um sistema, que pode ser explorada por uma ameaça [11]. Ataque é a tentativa de explorar uma vulnerabilidade e ganhar acesso não autorizado [15]. *Exploit* é um programa que tira vantagem de uma vulnerabilidade, com o objetivo de realizar um ataque bem-sucedido[28]. Os *exploits* são utilizados para executar comandos maliciosos.

Dentre os tipos de ataques mais comuns, estão o *phishing*, que é um crime cibernético em que os criminosos tentam obter informações confidenciais fingindo ser entidades confiáveis, como bancos ou empresas online, com o objetivo de enganar as vítimas para obter dados e realizar ações prejudiciais. [1]; o DoS (*Denial of Service*s [30] que é um ataque que visa tornar um serviço indisponível sobrecarregando seus recursos com tráfego excessivo, tornando-o inacessível para usuários legítimos. Uma inundação em um sistema de informação pode causar danos inimagináveis e deve ser evitada [24]. Novos sistemas e ambientes mais complexos e integrados desafiam a capacidade das organizações de garantirem segurança e qualidade de serviço [36]. A evolução constante da paisagem cibernética exige estratégias de segurança robustas e atualizações contínuas, destacando a importância da conscientização, educação e colaboração entre profissionais de segurança [13].

A compreensão desses conceitos é fundamental para aprimorar as estratégias de segurança. [33]. Os *pentests* seguem metodologias bem definidas, como a Metodologia de *Standard Penetration Testing Methodology* (PTES). Essas metodologias permitem uma avaliação proativa da segurança, como discutido em [29].

2.2 Trabalhos Relacionados

Segundo Almubairik e Wills [21], o *pentest* simula ações de *hackers* maliciosos. Um *hacker* ético, ou um *pentester*, realiza as ações com o consentimento de uma empresa contratante. O crime cibernético tem como objetivo causar danos e o *pentest* identifica falhas de segurança [17]. A metodologia PTES (Penetration Testing Execution Standard) é um padrão para a realização de *pentest*. A metodologia PTES engloba desde a fase de planejamento até a identificação de vulnerabilidades e a exploração de falhas de segurança. Ao seguir a PTES, os profissionais de segurança, normalmente terceirizados, têm um roteiro organizado para conduzir os testes [40].

Tramonto [5] e STRIDE (*Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege*) [20], são referências da literatura, metodologias de busca por ameaças. A metodologia Tramonto consiste em recomendações para testes de segurança. Tramonto é dividida em cinco etapas: Adequação, Verificação, Preparação, Execução e Finalização. Essas fases consistem em explorar possíveis vulnerabilidades de dados coletados. A metodologia STRIDE (*Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege*) [20] categoriza ameaças à segurança em seis tipos: *Spoofing* de identidade, *Tampering* de dados, *Repudiation* de origem, *Information disclosure*, *Denial of Service* e *Elevation of privilege*, cada um representando um tipo de ataque que pode comprometer a segurança.

Na seção 3, MAIA é detalhadamente descrita. MAIA, PTES e Tramonto apresentam alta capacidade de identificação de vulnerabilidades e alcançam alta precisão, ao passo que a STRIDE tem uma identificação mais limitada. MAIA é similar à Tramonto no sentido de explorar vulnerabilidades a partir de coleta de dados. Porém, MAIA vai adiante e calcula índices de exposição às vulnerabilidades coletadas, de maneira individual, para cada vulnerabilidade e, também, geral - um índice que engloba todos os impactos, na organização, de todas as vulnerabilidades encontradas. Em relação à precisão na avaliação do risco, MAIA e PTES superam STRIDE. Quanto à flexibilidade, facilidade e adaptabilidade, a MAIA se destaca. MAIA é a única metodologia que possui indicadores quantitativos do nível de risco associado às vulnerabilidades. MAIA também se destaca em

termos de custo, pois pode ser executada por equipes internas, enquanto as demais metodologias demandam empresas especializadas em *pentests*.

3 MAIA: Metodologia de Avaliação de Impactos de Ameaças a Sistemas de Informação

A metodologia científica empregada neste trabalho seguiu a abordagem da pesquisa qualitativa e quantitativa, com uma posição epistemológica positivista. O método de pesquisa-ação e o método de estudo de caso foram seguidos. A MAIA segue princípios da Teoria Geral dos Sistemas (TGS) [42] ao tratar sistemas de informação como entidades interconectadas, onde vulnerabilidades em um componente podem gerar impactos em todo o ecossistema. Essa abordagem sistêmica permite analisar a segurança de forma holística, considerando não apenas falhas técnicas, mas também seus efeitos sobre processos organizacionais e usuários.

A metodologia MAIA oferece uma abordagem sistemática para identificar vulnerabilidades em sistemas de informação. MAIA é baseada em técnicas, ferramentas e conceitos de *pentests*. A metodologia MAIA está alinhada a padrões internacionais de segurança da informação, como a ISO/IEC 27001 [8], que estabelece requisitos para a gestão de segurança da informação, e as diretrizes da OWASP [4], que identificam os principais riscos de segurança para aplicações web. Seu objetivo é desmistificar testes de invasão e tornar a prática de busca por vulnerabilidades periódica e corriqueira. Sua condução é flexível, adaptável e factível por equipes internas de empresas, sem a necessidade de contratação de empresas especialistas em *pentests*. Estruturada em fases, MAIA indica um conjunto de técnicas e ferramentas para cada etapa. Para a implementação eficaz da MAIA, a equipe precisa de acesso pleno às informações dos ativos da empresa, que incluem sistemas de informação, servidores, *websites* e outros elementos da infraestrutura. Ao ter uma visão completa dos ativos da empresa, a equipe pode identificar potenciais vulnerabilidades, fortalecendo a segurança cibernética.

Para a implementação da MAIA, a equipe deve ter acesso aos sistemas. É essencial que os profissionais envolvidos possuam conhecimentos básicos em segurança da informação e análise de vulnerabilidades. Treinamentos básicos são recomendados para garantir melhor compreensão dos processos e minimizar riscos operacionais.

As quatro fases de MAIA, coleta de informações, enumeração, exploração e análise de exposição de vulnerabilidade, serão detalhadas nas subseções a seguir.

3.1 Coleta de Informações

A fase de coleta de informações consiste na obtenção de dados disponíveis publicamente, também conhecidos como informações de fonte aberta (OSINT -*Open Source Intelligence*). Essas informações podem incluir registros de domínio, endereços IP, informações de contato, nomes de usuários, senhas e até mesmo arquivos confidenciais que foram inadvertidamente expostos online.

A coleta de informações na MAIA envolve pesquisas em bancos de dados públicos e análise de redes sociais. Isso é feito por meio de ferramentas como o *WebArchive*, que mantém registros históricos de páginas da web. Essas páginas podem conter informações sensíveis ou vulnerabilidades que não foram adequadamente protegidas ou removidas após a desativação do serviço. Outro aspecto importante é a busca por informações em fontes públicas, como redes sociais, fóruns online e bancos de dados de empresas. Essas fontes podem revelar vulnerabilidades de segurança nos sistemas ou na infraestrutura [12]. Os links para as ferramentas e um *checklist* sobre as fases da metodologia MAIA estão disponíveis em https://github.com/albanybar/MetodologiaMAIA.

3.2 Enumeração

Na fase de enumeração, é essencial explorar detalhes dos sistemas e da infraestrutura digital do alvo. Isso inclui mapear a topologia da rede e identificar possíveis pontos de entrada e vulnerabilidades. Ao utilizar técnicas como varreduras de portas e interações com serviços, é possível investigar a complexidade do ambiente em busca de falhas de configuração e inadequações que possam ser exploradas por invasores em potencial. Entre as atividades realizadas durante a enumeração, destaca-se a busca por diretórios e arquivos que possam estar publicamente acessíveis. Arquivos e diretórios expostos podem conter informações sensíveis ou até mesmo revelar vazamentos diretos de dados. As ferramentas de enumeração de DNS (*Domain Name System*), como dnsrecon[39] e dig[19], são amplamente utilizadas para descobrir registros DNS [37] e identificar ativos e possíveis vulnerabilidades. O Google Hacking [23] é uma técnica que usa operadores de pesquisa avançados no Google para encontrar informações sensíveis ou vulnerabilidades de segurança em sites e servidores. O WebArchive [41] é um serviço online que armazena versões antigas de páginas da web, permitindo aos usuários acessar conteúdo histórico da internet. Dirsearch [43] é uma ferramenta útil para enumeração de diretórios encontrados na WEB. O WhatWeb [38] é uma ferramenta valiosa para identificar as tecnologias web utilizadas em sites específicos, enquanto o Nmap [25] é fundamental para mapear redes e detectar possíveis vulnerabilidades. Durante a fase de enumeração, podem ser utilizados *scanners* de vulnerabilidades, que automatizam a busca por falhas de segurança em sistemas e servidores web. Um exemplo de *scanner* é o Nikto[6]. Ele é um *scanner* abrangente de vulnerabilidades para servidores web, que oferece uma análise detalhada das falhas de segurança presentes no sistema. O uso integrado e coordenado dessas ferramentas contribui significativamente para uma enumeração abrangente e precisa, permitindo uma análise eficaz do ambiente digital do alvo.

3.3 Exploração

Exploit é um programa que explora vulnerabilidades de sistemas ou de infraestruturas computacionais [3]. A execução de um *exploit* resulta em acesso ao sistema. A fase exploração envolve análise das vulnerabilidades mapeadas nas fases anteriores, fazendo uso de *exploits*, *scripts* personalizados e técnicas de injeção de código. O objetivo é não apenas explorar vulnerabilidades conhecidas, mas também compreender as interações complexas entre os diversos componentes do sistema. Isso permite a identificação de potenciais pontos de falha que poderiam ser explorados por invasores. A execução de *exploits* deve ser feita com cuidado e responsabilidade, pois pode causar danos não intencionais ao sistema. O Metasploit[32] se destaca como uma ferramenta poderosa que automatiza aspectos do processo de exploração, facilitando a execução de *exploits* e a validação rápida das vulnerabilidades identificadas.

3.4 Análise de Exposição de Vulnerabilidade

Na quarta e última fase, o foco é a quantificação do risco relacionado às vulnerabilidades individuais identificadas nas etapas precedentes. Essa fase é subdividida em duas etapas. Na primeira, é realizado o cálculo do Índice de Exposição de Vulnerabilidade (IEV) para cada vulnerabilidade identificada. Na segunda, é efetuado o cálculo do Índice de Exposição de Vulnerabilidade Geral (IEV_g), que possibilita a mensuração do risco de forma abrangente, considerando todas as vulnerabilidades encontradas. Os valores atribuídos dependem muito de aspectos organizacionais e até mesmo pessoais, pois referem-se à percepção de severidade de uma vulnerabilidade.

3.4.1 Etapa de Cálculo do Índice de Exposição de Vulnerabilidades. Na primeira etapa da quarta fase, é feito o cálculo do Índice de Exposição de Vulnerabilidades *IEV* para cada vulnerabilidade identificada. O *IEV* é composto por cinco categorias distintas. A cada categoria é atribuído um valor que corresponde à avaliação do risco associado, conforme explicado a seguir.

(1) Severidade da Vulnerabilidade (SV): Refere-se à gravidade do impacto que a exploração da vulnerabilidade encontrada pode causar no sistema. Vulnerabilidades com potencial para causar danos mais significativos são classificadas como mais severas. São atribuídos quatro níveis de severidade: Crítica (4), Alta (3), Média (2) e Baixa (1). Caso a organização siga um *CVE (Common Vulnerabilities and Exposures)*[26], pode se basear em seus valores.
(2) Potencial de Exploração (PE): Indica a facilidade ou a dificuldade em explorar a vulnerabilidade. Quanto mais fácil for para explorar a vulnerabilidade, maior será o potencial de exploração. Os níveis são: Alto (4), Médio (3), Baixo (2) e Não Explorado (1).
(3) Impacto do Ataque (IA): Avalia os efeitos adversos que podem ocorrer se a vulnerabilidade for explorada com sucesso. Isso inclui danos à integridade, à confidencialidade ou à disponibilidade dos dados e dos sistemas. Os níveis de impacto são: Alto (4), Médio (3), Baixo (2) e Impacto Mínimo (1).
(4) Mitigação Disponível (MD): Refere-se à eficácia das medidas de mitigação existentes para reduzir ou eliminar o risco associado à vulnerabilidade. Quanto mais eficazes forem as contramedidas disponíveis, menor será o risco. Esta categoria considera o esforço necessário para corrigir a vulnerabilidade. Os níveis são: Nenhuma Mitigação (4), Mitigação Temporária (3), Correção Complexa (2) e Correção Simples (1).
(5) Probabilidade de Ocorrência (PO): Estima a probabilidade de um ataque bem-sucedido contra a vulnerabilidade. Isso pode ser influenciado por vários fatores, como a visibilidade da vulnerabilidade, o perfil do atacante e a maturidade das defesas. Baseando-se na probabilidade de um ataque ocorrer, utilizando o OWASP |(*Open Source Foundation for Application Security*) Top 10 como referência. Os níveis são: Muito Provável (4), Provável (3), Pouco Provável (2) e Raro (1)

A equação 1 mostra que o *IEV* calculado, para cada vulnerabilidade encontrada, corresponde à soma da severidade de vulnerabilidade (SV) com o potencial de exploração (PE), com o impacto do ataque (IA), com a mitigação disponível (MD) e com a probabilidade de ocorrência (PO). A equação 1 fornece uma medida quantitativa para avaliar o nível de exposição associado a uma vulnerabilidade específica.

$$IEV = SV + PE + IA + MD + PO \tag{1}$$

3.4.2 Etapa de Cálculo do Índice Geral de Exposição de Vulnerabilidade. Na segunda etapa da quarta fase, o Índice Geral de Exposição de Vulnerabilidade (IEV_g) é calculado. Essa é uma métrica crucial na metodologia MAIA, pois fornece uma noção do grau do risco geral associado às várias vulnerabilidades identificadas durante as fases anteriores. Essa métrica é calculada considerando não apenas a gravidade individual de cada vulnerabilidade, mas também o número de ocorrências de cada uma delas. Os quantificadores IEV e IEV_g não são propostos para análise de risco ou para comparação de riscos entre empresas e sim para indicar o grau de gravidade das vulnerabilidades encontradas. Os critérios avaliados por esses indicadores são específicos de cada empresa, uma vez que cada cenário empresarial é único e o impacto ou a correção de uma vulnerabilidade difere de empresa para empresa. Existe uma possibilidade significativa de que dois analistas de segurança de empresas diferentes atribuam níveis diferentes, na etapa anterior, para as mesmas vulnerabilidades. A quantificação visa apontar existências de riscos causados por vulnerabilidades expostas, identificadas por MAIA, na organização alvo. A organização/empresa poderá ter um histórico de realizações da metodologia MAIA, permitindo uma análise relativa e contextualizada de vulnerabilidades encontradas, ao longo do tempo. Utilizar o IEV e o (IEV_g) para análises de risco ou para comparações com outras empresas pode levar a interpretações inadequadas e conclusões incorretas, pois os parâmetros e contextos são distintos em cada caso. Os índices propostos visam alertar sobre a gravidade de vulnerabilidades encontradas.

A fórmula do IEV_g é expressa de acordo com a equação 2. Nela, o termo IEV_i denota o *IEV* da i-ésima vulnerabilidade. O termo $Ocorrencia_i$ indica a quantidade de vezes que essa vulnerabilidade foi detectada. O termo $\sum_{i=1}^{n} Ocorrencia_i$ representa o número total de ocorrências de vulnerabilidades.

$$IEV_g = \frac{\sum_{i=1}^{n}(IEV_i * Ocorrencia_i)}{\sum_{i=1}^{n} Ocorrencia_i} \tag{2}$$

A contagem de ocorrências é realizada separadamente para cada tipo de vulnerabilidade, visando uma avaliação precisa. Por exemplo, se 13 senhas forem encontradas em um diretório exposto, essa constatação será considerada como uma única ocorrência no cálculo do índice geral, independentemente do número total de senhas identificadas. Essa abordagem reflete uma análise ponderada que leva em consideração tanto a severidade quanto a frequência das vulnerabilidades, proporcionando uma métrica abrangente para avaliação do risco global no ambiente analisado. O IEV_g varia de 5 a 20, conforme ilustrado na Figura 1. Na escala, 0 é o valor para o ambiente mais seguro e 20 é o valor para o ambiente extremamente vulnerável. Esses valores correspondem às somas mínima e máxima dos índices individuais.

A avaliação das vulnerabilidades na metodologia MAIA deve ser realizada por profissionais de segurança da informação da organização ou por um comitê interno de segurança. Recomenda-se que

múltiplos profissionais participem da atribuição de valores ao IEV e IEVg para mitigar subjetividades. Em cenários onde a equipe de segurança é reduzida, a organização pode recorrer a benchmarks de vulnerabilidades conhecidas como CVSS [34] e OWASP [4] Top 10 para auxiliar na categorização dos riscos.

4 Estudo de Caso, Resultados e Análises

Esta seção apresenta os resultados obtidos a partir da aplicação da metodologia MAIA em uma organização real. O ambiente de produção dos sistemas de informação da empresa é dinâmico e complexo. A empresa tem múltiplos sistemas interconectados em constante atividade. Durante o teste, foi necessário lidar com a diversidade de tecnologias, protocolos e configurações, o que demandou uma abordagem adaptável. É importante ressaltar que, para preservar a segurança e a confidencialidade da organização, todos os dados obtidos foram rigorosamente anonimizados. Qualquer referência específica à empresa foi omitida ou substituída por dados fictícios, garantindo que nenhum dado sensível esteja exposto. Os resultados mostrados refletem exclusivamente as vulnerabilidades identificadas, sem expor qualquer informação sensível ou confidencial da organização. A generalização dos resultados para outras empresas não deve ser feita, devido às especificidades de cada ambiente e infraestrutura de TI. Os resultados estão organizados de acordo com as fases distintas da metodologia conforme a Seção 3.

O estudo de caso foi realizado em uma organização do setor governamental, abrangendo a análise de vulnerabilidades em sistemas de informação voltados para serviços governamentais. Esses sistemas possuem integração entre si, com comunicação ativa entre diferentes plataformas e acesso a bases de dados. Alguns sistemas são exclusivos para usuários internos, enquanto outros também são acessados por usuários externos, ampliando a superfície de exposição a possíveis ameaças.

4.1 Fase 1: Coleta de Informações

Na coleta de informações, destacaram-se duas ferramentas que desempenharam papéis distintos, mas complementares: o Google Hacking [23] e o WebArchive[41].

O Google Hacking [23] é uma técnica que usa operadores de pesquisa avançados no Google para encontrar informações sensíveis ou vulnerabilidades de segurança em sites e servidores. O WebArchive é um serviço online que armazena versões antigas de páginas da web, permitindo aos usuários acessar conteúdo histórico da internet. A Figura 2 ilustra a aplicação do Google Hacking [23] , que se revelou eficaz na localização de arquivos contendo informações sensíveis, como usuários e senhas. Por sua vez, a Figura 3 representa a utilização do WebArchive, uma ferramenta crucial para a obtenção de informações publicamente acessíveis na web, focando especialmente na identificação de e-mails associados à infraestrutura inspecionada.

Através da aplicação da técnica de busca de e-mails indexados pelo WebArchive, como ilustrado na Figura 2, foi possível identificar e-mails de usuários associados à organização.

4.2 Fase 2 Enumeração

Na transição para a fase de enumeração, a atenção se volta para uma análise detalhada e sistemática da infraestrutura identificada na etapa anterior de coleta de informações. Nessa fase, almeja-se obter um panorama mais aprofundado do alvo, identificando ativos, serviços ativos e possíveis vulnerabilidades. A empresa, com sua complexidade e diversidade de tecnologias em uso, proporciona um ambiente desafiador e dinâmico para a aplicação da metodologia, exigindo uma abordagem adaptativa para lidar com a variedade de sistemas interconectados e em constante atividade. A enumeração emerge como um estágio estratégico para mapear a superfície inspecionada, permitindo uma análise mais precisa e direcionada das potenciais áreas de fragilidade nos sistemas sob avaliação. Neste cenário, a metodologia MAIA busca destacar sua eficácia na identificação de informações cruciais que fundamentarão as etapas subsequentes do processo de avaliação de segurança. Os resultados dessa fase revelaram a detecção de páginas de *logs*, contendo informações sensíveis que poderiam ser alvos de invasores, além de página contendo configurações da rede interna. Ao realizar a enumeração dos diretórios com o uso do Dirsearch [43], foram identificadas pastas contendo arquivos de *logs* expostos.

Vale ressaltar que algumas informações foram omitidas para preservar a confidencialidade e segurança da instituição. A Figura 2 ilustra visualmente esse processo. A imagem presente na Figura 4 ilustra a exposição pública de uma pasta de arquivos de *logs*, que foi identificada utilizando uma ferramenta de enumeração de diretórios, como o Dirsearch.

Na fase de enumeração, não apenas diretórios foram identificados, mas também arquivos, como o "info.php", que foi identificado como exposto, revelando informações confidenciais, conforme ilustrado na Figura 5.

A vulnerabilidade denominada *"Git Exposed"* refere-se à exposição do diretório ".git", revelando informações sensíveis sobre algum repositório do tipo Git (por exemplo em github.com) associado ao projeto conforme Figura 6. Ao identificar o diretório ".git" como público, essa situação pode representar uma ameaça à segurança, uma vez que informações cruciais, como histórico de *commits*, configurações de projeto e, em alguns casos, credenciais sensíveis, podem ser acessadas indevidamente por usuários não autorizados. Essa vulnerabilidade pode ser explorada por potenciais invasores para obter *insights* sobre códigos-fonte de projetos organizacionais, identificar possíveis falhas de segurança ou até mesmo realizar alterações não autorizadas no repositório. No caso da empresa alvo, essa falha foi encontrada durante a fase de enumeração, evidenciando a importância de identificar e corrigir esse tipo de exposição em ambientes digitais corporativos.

4.3 Exploração

As vulnerabilidades identificadas durante as fases anteriores são exploradas, na terceira fase. Nela, são utilizadas abordagens manuais e automatizadas para verificar a possibilidade de exploração efetiva das vulnerabilidades descobertas. Essa fase visa compreender as vulnerabilidades e suas implicações e, quando necessário, realizar testes para validar a presença e extensão dos riscos associados. A exploração ética dessas vulnerabilidades é fundamental para entender a exposição real do sistema, permitindo que medidas corretivas sejam adotadas para fortalecer a segurança da infraestrutura avaliada.

Figure 1: Escala de gravidade do risco geral para o IEVg calculado

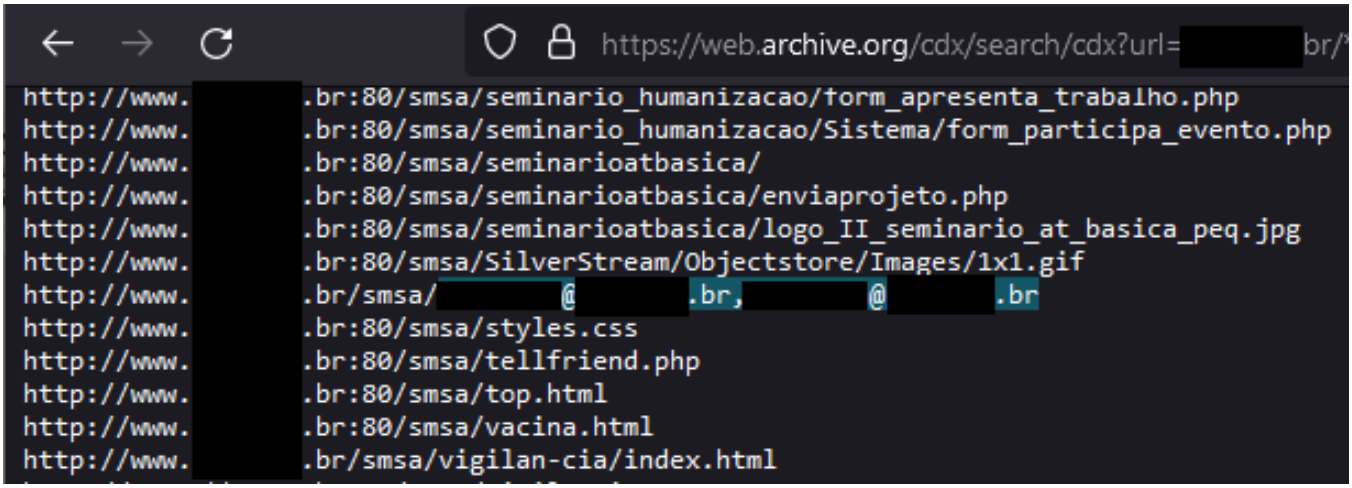

Figure 2: E-mails encontrados no WebArchive

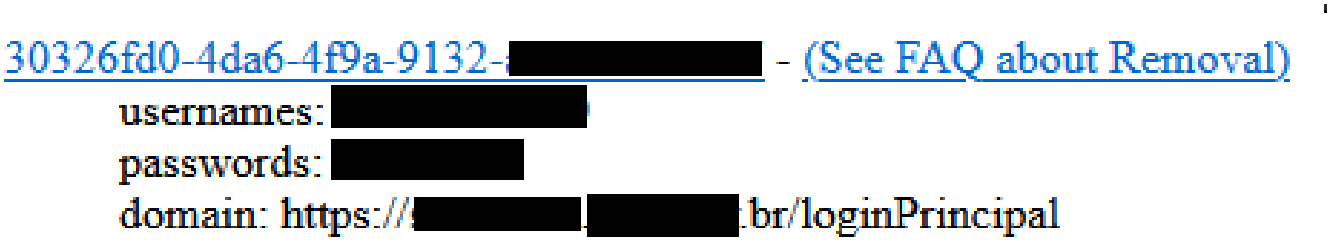

Figure 3: Dados encontrados com Google Hacking.

Destaca-se a abordagem manual para explorar a vulnerabilidade identificada anteriormente como *"Git Exposed"*. Essa vulnerabilidade, que envolve a exposição do diretório ".git", foi identificada durante a fase de enumeração, revelando informações sensíveis associadas ao repositório Git. A exploração manual dessa falha inclui a análise detalhada do conteúdo exposto no diretório ".git", buscando por informações relevantes, como credenciais, configurações de projeto e histórico de *commits*. Como mostram as Figuras 7 e 8, foi possível identificar usuários e senhas de sistemas internos em arquivos no diretório .git.

As credenciais obtidas por meio da técnica de *Google Hacking* foram submetidas à validação durante a fase de exploração. Foram feitos acessos ao sistema da empresa, com sucesso, com as credenciais encontradas. Porém, por uma questão de privacidade da empresa, os mesmos estão ocultos, aqui. O processo de exploração permitiu verificar a autenticidade das credenciais, validando a relevância das informações coletadas.

4.4 Análise de Exposição de Vulnerabilidade

Na fase de análise de exposição de vulnerabilidade, é realizada uma avaliação de dados obtidos nas fases anteriores. É feita a categorização das vulnerabilidades conforme sua gravidade e a quantificação das potenciais ameaças que podem ser exploradas. MAIA classifica e prioriza as vulnerabilidades de acordo com seu impacto potencial, possibilitando a definição de estratégias de mitigação eficazes. A análise de exposição de vulnerabilidade fornece direcionamentos aos responsáveis pela segurança, através da indicação quantitativa quanto ao nível de gravidade de exposição de vulnerabilidades.

Foram identificadas cinco vulnerabilidades no ambiente da empresa alvo do estudo de caso. O Índice de Exposição de Vulnerabilidade (IEV) foi calculado para cada uma delas. Cada IEV reflete a soma dos critérios estabelecidos nas categorias de Potencial de Exploração, Impacto do Ataque, Mitigação Disponível, Probabilidade de Ocorrência e Severidade da Vulnerabilidade. A análise resultou em valores específicos para cada vulnerabilidade, refletindo o risco

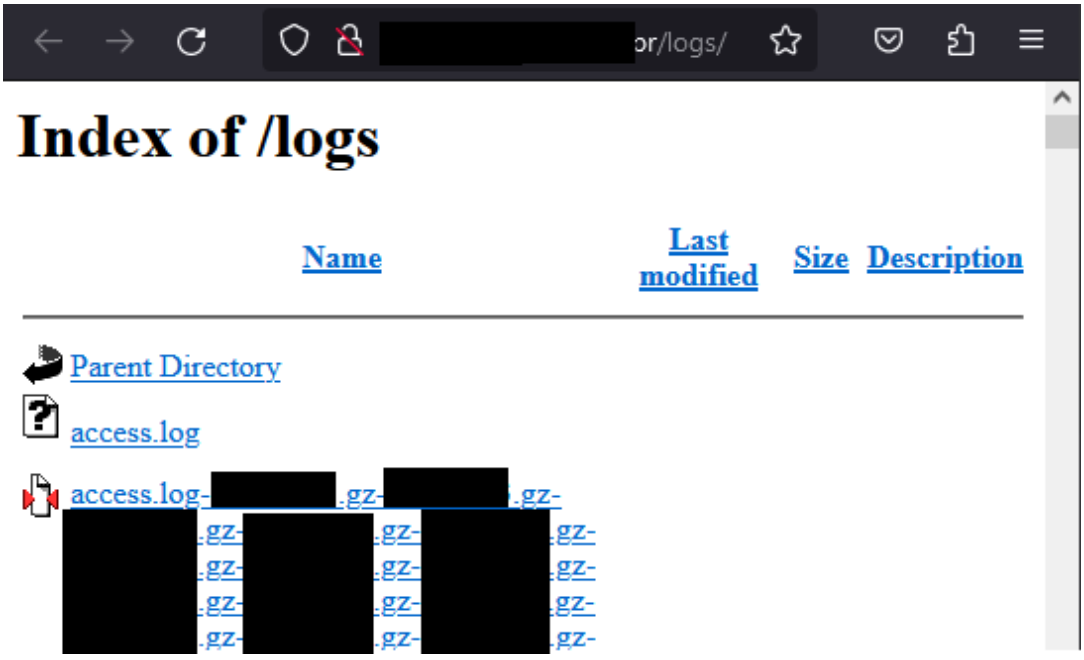

Figure 4: Pasta de *logs* exposta.

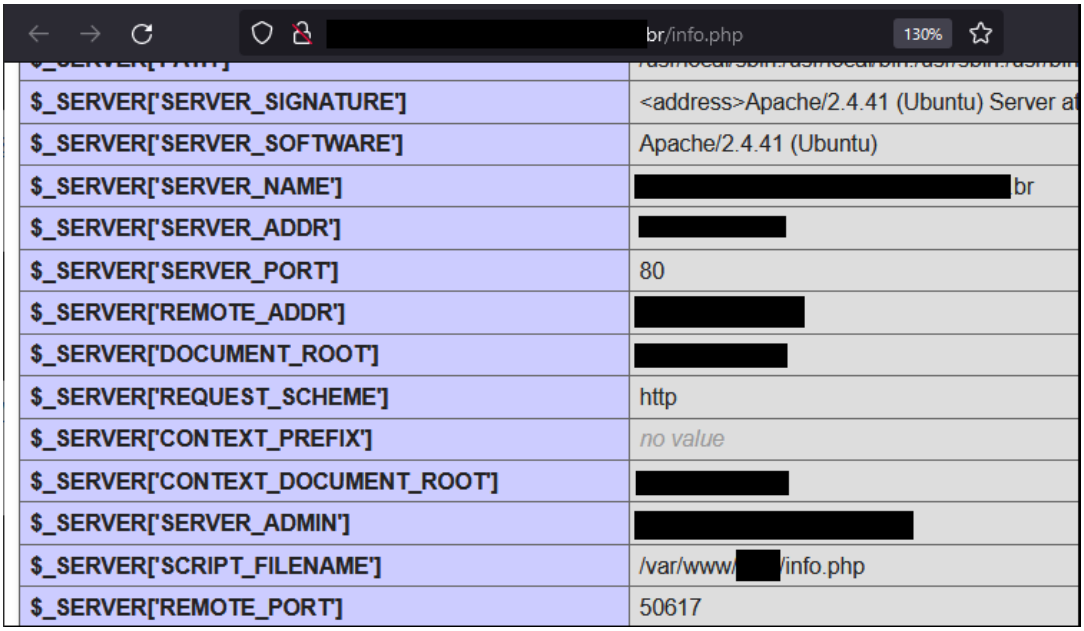

Figure 5: Arquivo info.php exposto

associado a cada uma das vulnerabilidades encontradas, enumeradas a seguir. Os valores foram atribuídos pelo responsável pela segurança dos sistemas da empresa, auxiliado pelos autores deste trabalho. Os critérios de atribuição de valores, portanto, são pessoais e subjetivos. Eles dependem do contexto das empresas e da visão dos administradores dos sistemas.

(1) Email Indexado em Webarchive (1 Ocorrência):
- Severidade da Vulnerabilidade: Média (2)
- Potencial de Exploração: Alto (4)
- Impacto do Ataque: Baixo (2)
- Mitigação Disponível: Simples (1)
- Probabilidade de Ocorrência: Provável (3)

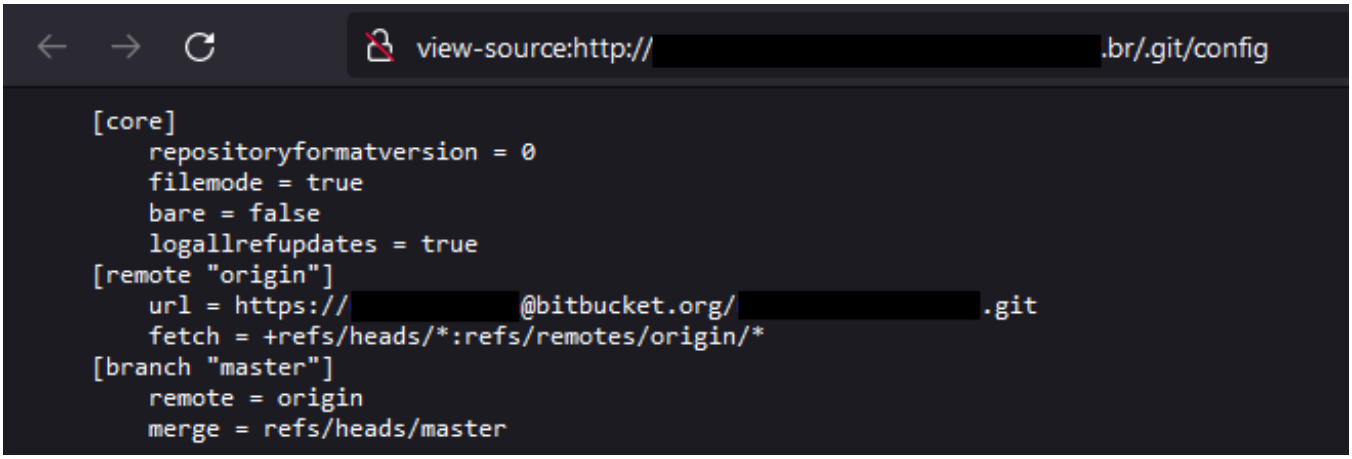

Figure 6: Diretório .git exposto

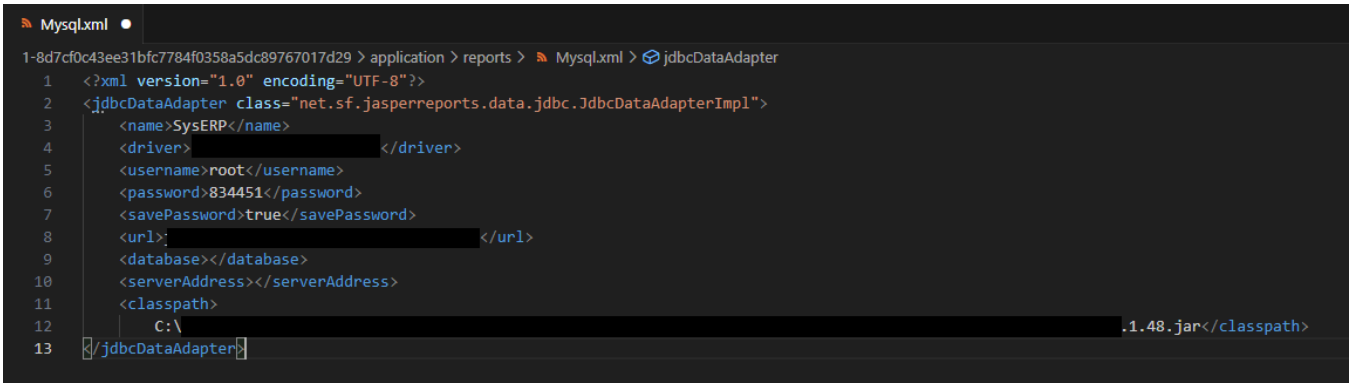

Figure 7: Arquivo contendo credenciais no diretório .git

Figure 8: Arquivo contendo credenciais no diretório .git

$$IEV = 2 + 4 + 2 + 1 + 3 = 12 \quad (3)$$

(2) Credenciais encontradas com *Google Hacking* (3 Ocorrências):
- Severidade da Vulnerabilidade: Média (2)
- Potencial de Exploração: Alto (4)
- Impacto do Ataque: Médio (3)
- Mitigação Disponível: Simples (1)
- Probabilidade de Ocorrência: Provável (3)

$$IEV = 2 + 4 + 3 + 1 + 3 = 13 \quad (4)$$

(3) Diretórios de *Logs* Expostos (2 Ocorrências):
- Severidade da Vulnerabilidade: Crítica (4)
- Potencial de Exploração: Alto (4)
- Impacto do Ataque: Alto (4)
- Mitigação Disponível: Simples (1)
- Probabilidade de Ocorrência: Provável (3)

$$IEV = 4 + 4 + 4 + 1 + 3 = 16 \quad (5)$$

(4) Arquivo de Configuração Exposto (1 Ocorrência):
- Severidade da Vulnerabilidade: Alta (3)
- Potencial de Exploração: Alto (4)
- Impacto do Ataque: Alto (4)
- Mitigação Disponível: Simples (1)
- Probabilidade de Ocorrência: Provável (3)

$$IEV = 3 + 4 + 4 + 1 + 3 = 15 \quad (6)$$

(5) Diretório .git Exposto (2 Ocorrências):
- Severidade da Vulnerabilidade: Crítica (4)
- Potencial de Exploração: Alto (4)
- Impacto do Ataque: Alto (4)
- Mitigação Disponível: Simples (1)
- Probabilidade de Ocorrência: Provável (3)

$$IEV = 4 + 4 + 4 + 1 + 3 = 17 \quad (7)$$

O IEV_g foi calculado considerando a média ponderada dos IEVs de todas as vulnerabilidades. A ponderação é proporcional ao número de ocorrências da respectiva vulnerabilidade. O cálculo resultou em um valor de $IEVg$ igual a 14,6 como mostra a equação 8. Esse valor de $IEVg$ indica um alto risco para o sistema analisado. A escala do IEV_g vai de 0 até 20 está ilustrada na Figura 9. O valor 14,6 indica um nível alto de risco. O valor, obtido por meio da análise ponderada de várias vulnerabilidades, aponta para a presença de ameaças consideráveis que demandam atenção imediata.

$$IEV_g = (12*1+13*3+16*2+15*1+17*2)/(1+3+2+1+2) = 14,6 \quad (8)$$

Os achados obtidos com a aplicação da metodologia MAIA demonstram a sua eficácia na identificação e quantificação de vulnerabilidades de segurança. A análise dos índices de exposição (IEV e IEVg) permitiu que a organização avaliada tivesse uma visão quantitativa do risco associado às vulnerabilidades encontradas. Esse resultado é um avanço em relação a metodologias tradicionais que não fornecem métricas quantitativas tão acessíveis. Em relação ao estado da arte, a MAIA se destaca por ser uma alternativa aos *pentests* tradicionais, que exigem equipes altamente especializadas e podem ter custos elevados. Diferentemente de metodologias como PTES e STRIDE, a MAIA incorpora um índice de exposição de vulnerabilidades, permitindo priorização de riscos.

Uma das limitações do estudo de caso é a subjetividade na avaliação das vulnerabilidades, uma vez que os critérios do IEV são baseados na percepção dos analistas de segurança. Para mitigar essa questão, recomenda-se que a avaliação seja conduzida por múltiplos profissionais, permitindo uma visão mais equilibrada do risco.

5 Conclusão

Como principal contribuição à comunidade de sistemas de informação, a metodologia MAIA emerge como uma abordagem alternativa a *pentests* tradicionais, para a inspeção e descoberta de vulnerabilidades. As fases de coleta de informações, enumeração, exploração e análise de exposição de vulnerabilidade possibilitam descobertas de falhas de segurança e a quantificação de índices de vulnerabilidade que indicam níveis de alerta e necessidades de ações rápidas. A execução interna da metodologia, com a colaboração de equipes multidisciplinares, pode proporcionar uma compreensão profunda da infraestrutura, dos processos internos da organização e dos riscos aos mesmos. Decisões assertivas quanto à correção de vulnerabilidades críticas podem ser tomadas a partir dos resultados de MAIA. MAIA é única metodologia que possui indicadores (*IEV* e *IEVg*) quantitativos de nível de risco associado às vulnerabilidades. Os índices calculados englobam níveis de severidade das vulnerabilidades, potenciais de exploração e impactos de um ataque. A metodologia MAIA pode ser executada por equipes internas, enquanto as demais metodologias demandam empresas especializadas em *pentests*.

É importante ressaltar, como limitação, que a MAIA, ao apontar índices de vulnerabilidades associados às ameaças, não fornece diretamente orientações específicas sobre soluções para os problemas identificados. Este aspecto destaca a necessidade de abordagens complementares para a mitigação eficaz de riscos cibernéticos. Dessa forma, a MAIA se apresenta como uma metodologia para fortalecer a segurança cibernética, identificando possíveis vazamentos de dados, oferecendo uma quantificação das vulnerabilidades, indicando a gravidade e a necessidade de priorização na mitigação de riscos. A metodologia MAIA representa uma contribuição para a gestão proativa da segurança de sistemas da informação, especialmente em um cenário de constante evolução tecnológica e de crescente exposição a ameaças cibernéticas.

Além de oferecer uma alternativa prática aos *pentests* tradicionais, a metodologia MAIA contribui para a segurança da informação em sistemas organizacionais, abordando desafios como a acessibilidade de metodologias para análise de vulnerabilidades e a necessidade de soluções adaptáveis a diferentes contextos. Sua abordagem estruturada favorece a identificação e a quantificação de riscos, permitindo que organizações aprimorem suas estratégias de defesa cibernética sem depender exclusivamente de avaliações externas. Dessa forma, a MAIA incentiva a adoção de práticas sistemáticas de segurança aos sistemas de informação, alinhadas às exigências de confiabilidade, integridade e proteção dos dados em ambientes corporativos e governamentais.

Como sugestões para trabalhos futuros, é interessante repetir a utilização de MAIA em outros estudos de caso e considerar a elaboração de diretrizes ou estratégias práticas para implementar recomendações que possam ser fornecidas por MAIA.

Acknowledgments

The authors would like to thank the Minas Gerais Research Support Foundation – Fapemig (Project CEX APQ 04034-23), the Coordination for the Improvement of Higher Education Personnel – CAPES – (Master's scholarship through the Postgraduate Support Program for Community Higher Education Institutions (PROSUC/CAPES),

Figure 9: Resultado $IEVg$ em escala de gravidade do risco geral da empresa

Project PROAP 88887.842889/2023-00 – PUC/MG, Project PDPG 88887.708960/2022-00 – PUC/MG - INFORMATICS Finance Code 001),and Pontifical Catholic University of Minas Gerais (PUC Minas).

References

[1] Ahmed Aleroud and Lina Zhou. 2017. Phishing environments, techniques, and countermeasures: A survey. *Computers & Security* 68 (2017), 160–196.

[2] Taylor Armerding. 2018. The 17 biggest data breaches of the 21st century. *CSO online* 26 (2018).

[3] Ömer Aslan, Semih Serkant Aktuğ, Merve Ozkan-Okay, Abdullah Asim Yilmaz, and Erdal Akin. 2023. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics* 12, 6 (2023). https://doi.org/10.3390/electronics12061333

[4] Matthew Bach-Nutman. 2020. Understanding the top 10 owasp vulnerabilities. *arXiv preprint arXiv:2012.09960* (2020).

[5] Daniel Dalalana Bertoglio and Avelino Francisco Zorzo. 2016. Tramonto: Uma estratégia de recomendações para testes de penetração. In *Anais do XVI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. SBC, 366–379.

[6] Chris Binnie and Rory McCune. 2021. Server Scanning With Nikto. (2021).

[7] Kevin Cardwell. 2016. *Building Virtual Pentesting Labs for Advanced Penetration Testing*. Packt Publishing Ltd.

[8] Giovanna Culot, Guido Nassimbeni, Matteo Podrecca, and Marco Sartor. 2021. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal* 33, 7 (2021), 76–105.

[9] Lucas Soares Da-Silva, Carlos Renato Storck, Ivan Fontainha de Alvarenga, Thiago Augusto Alves, and Fátima de Lima Procópio Duarte-Figueiredo. 2025. Local 5G and 6G micro-operators for new business models: a systematic literature review. *OBSERVATÓRIO DE LA ECONOMÍA LATINOAMERICANA* 23, 2 (fev. 2025), e9023. https://doi.org/10.55905/oelv23n2-088

[10] Lucas Soares Da-Silva, Carlos Renato Storck, and Fatima de LP Duarte-Figueiredo. 2019. A Dynamic Load Balancing Algorithm for Data Plane Traffic.. In *LANOMS*.

[11] Yuri Diógenes and Daniel Mauser. 2016. *Certificação Security+: da prática para o exame SYO-401*. Novaterra Editora e Distribuidora LTDA.

[12] Simon Donig, Markus Eckl, Sebastian Gassner, and Malte Rehbein. 2023. Web archive analytics: Blind spots and silences in distant readings of the archived web. *Digital Scholarship in the Humanities* 38, 3 (04 2023), 1033–1048. https://doi.org/10.1093/llc/fqad014 arXiv:https://academic.oup.com/dsh/article-pdf/38/3/1033/51309560/fqad014.pdf

[13] Fábio Coutinho dos Santos, Fátima Duarte-Figueiredo, Robson E. De Grande, and Aldri L. dos Santos. 2024. Enhancing a fog-oriented IoT authentication and encryption platform through deep learning-based attack detection. *Internet of Things* 27 (2024), 101310. https://doi.org/10.1016/j.iot.2024.101310

[14] Asligul Erkan-Barlow, Thanh Ngo, Rajni Goel, and Denise W Streeter. 2023. An in-depth analysis of the impact of cyberattacks on the profitability of commercial banks in the United States. *Journal of Global Business Insights* 8, 2 (2023), 120–135.

[15] Ajinkya A Farsole, Amurta G Kashikar, and Apurva Zunzunwala. 2010. Ethical hacking. *International Journal of Computer Applications* 1, 10 (2010), 14–20.

[16] F. Duarte Figueiredo and A. Loureiro. 2004. DiffMobil–Uma Arquitetura de Qualidade de Serviço Fim-a-Fim em Redes GPRS. In *Tese de Doutorado*, Universidade Federal de Minas Gerais (Ed.). Departamento de Ciência da Computação.

[17] Mohamed C Ghanem and Thomas M Chen. 2019. Reinforcement learning for efficient network penetration testing. *Information* 11, 1 (2019), 6.

[18] Diptiben Ghelani. 2022. Cyber security, cyber threats, implications and future perspectives: A Review. *Authorea Preprints* (2022).

[19] Liz Izhikevich, Gautam Akiwate, Briana Berger, Spencer Drakontaidis, Anna Ascheman, Paul Pearce, David Adrian, and Zakir Durumeric. 2022. ZDNS: a fast DNS toolkit for internet measurement. In *Proceedings of the 22nd ACM Internet Measurement Conference*. 33–43.

[20] Tomoko Kaneko, Yuji Takahashi, Takao Okubo, and Ryoichi Sasaki. 2018. Threat analysis using STRIDE with STAMP/STPA. In *The international workshop on evidence-based security and privacy in the wild*. 10–17.

[21] Rajiv Kumar and Katlego Tlhagadikgora. 2019. Internal network penetration testing using free/open source tools: Network and system administration approach. In *Advanced Informatics for Computing Research: Second International Conference, ICAICR 2018, Shimla, India, July 14–15, 2018, Revised Selected Papers, Part II 2*. Springer, 257–269.

[22] Yuchong Li and Qinghui Liu. 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports* 7 (2021), 8176–8186.

[23] Johnny Long, Bill Gardner, and Justin Brown. 2011. *Google hacking for penetration testers*. Vol. 2. Elsevier.

[24] Efrem Eladie de Oliveira Lousada and Fátima de Lima Procópio Duarte Figueiredo. 2024. CN-ffVP: uma solução para mitigação de tempestade de broadcast baseada em métricas de redes complexas, distância e energia dos nos. *OBSERVATÓRIO DE LA ECONOMÍA LATINOAMERICANA* 22, 1 (jan. 2024), 4494–4512. https://doi.org/10.55905/oelv22n1-237

[25] Gordon Fyodor Lyon. 2009. *Nmap network scanning: The official Nmap project guide to network discovery and security scanning*. Insecure.

[26] Peter Mell and Tim Grance. 2002. Use of the common vulnerabilities and exposures (cve) vulnerability naming scheme. *NIST Special Publication* 800 (2002), 51.

[27] Daniel Moreno. 2016. *Pentest em redes sem fio*. Novatec Editora.

[28] Marcin Nawrocki, Matthias Wählisch, Thomas C Schmidt, Christian Keil, and Jochen Schönfelder. 2016. A survey on honeypot software and data analysis. *arXiv preprint arXiv:1608.06249* (2016).

[29] Chris Nickerson, Dave Kennedy, E Smith, A Rabie, S Friedli, J Searle, B Knight, C Gates, and J McCray. 2014. Penetration testing execution standard. *URL: http://www. pentest-standard. org* (2014).

[30] Sean-Philip Oriyano. 2016. *CEH v9: Certified Ethical Hacker Version 9 Study Guide*. John Wiley & Sons.

[31] Gaetano Perrone, Simon Pietro Romano, Nicola d'Ambrosio, and Vittoria Pacchiano. 2024. Unleashing Exploit-Db Data for the Automated Exploitation of Intentionally Vulnerable Docker Containers. *Available at SSRN 4779063* (2024).

[32] Sudhanshu Raj and Navpreet Kaur Walia. 2020. A Study on Metasploit Framework: A Pen-Testing Tool. In *2020 International Conference on Computational Performance Evaluation (ComPE)*. 296–302. https://doi.org/10.1109/ComPE49325.2020.9200028

[33] Fatima Salahdine and Naima Kaabouch. 2019. Social engineering attacks: A survey. *Future internet* 11, 4 (2019), 89.

[34] Karen Scarfone and Peter Mell. 2009. An analysis of CVSS version 2 vulnerability scoring. In *2009 3rd International Symposium on Empirical Software Engineering and Measurement*. IEEE, 516–525.

[35] Carlos R. Storck, Efrem E. de O. Lousada, Guilherme G. de O. Silva, Raquel A.F. Mini, and Fátima Duarte-Figueiredo. 2021. FiVH: A solution of inter-V-Cell handover decision for connected vehicles in ultra-dense 5G networks. *Vehicular Communications* 28 (2021), 100307. https://doi.org/10.1016/j.vehcom.2020.100307

[36] Carlos Renato Storck and Fátima Duarte-Figueiredo. 2020. A Performance Analysis of Adaptive Streaming Algorithms in 5G Vehicular Communications in Urban Scenarios. In *2020 IEEE Symposium on Computers and Communications (ISCC)*. 1–7. https://doi.org/10.1109/ISCC50000.2020.9219682

[37] A. Tanenbaum, D. Wetherall, and N. Feamster. 2021. Computer Networks. In *Book*, Pearson (Ed.). Education Limited.

[38] Aan Fleur Terrens, Sze-Ee Soh, and Prue Morgan. 2022. What web-based information is available for people with Parkinson's disease interested in aquatic physiotherapy? A social listening study. *BMC neurology* 22, 1 (2022), 170.

[39] Matt Tigner, Hayden Wimmer, and Carl M Rebman. 2021. Analysis of kali linux penetration tools: A survey of hacking tools. In *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)*. IEEE, 1–6.

[40] Ferzha Putra Utama and Raden Muhammad Hilmi Nurhadi. 2024. Uncovering the Risk of Academic Information System Vulnerability through PTES and OWASP Method. *CommIT (Communication and Information Technology) Journal* 18, 1 (2024). https://doi.org/10.21512/commit.v18i1.9384

[41] Michael Völske, Janek Bevendorff, Johannes Kiesel, Benno Stein, Maik Fröbe, Matthias Hagen, and Martin Potthast. 2021. Web archive analytics. *arXiv preprint arXiv:2107.00893* (2021).

[42] Ludwig Von Bertalanffy. 1950. An outline of general system theory. *The British Journal for the Philosophy of science* 1, 2 (1950), 134–165.

[43] Asriza Yolanda and Cutifa Safitri. 2023. Analyzing Proxychains Traffic on the Pentest Scenario: Enhancements in Network Forensics through Wireshark. In *2023 International Conference on Information Technology and Computing (ICITCOM)*. IEEE, 340–345.

Received 22 November 2024; revised 4 February 2025; accepted 12 March 2025