Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Lucas Harteman

FORTALECIMENTO DA SEGURANÇA DA INFORMAÇÃO EM PMES POR MEIO DO PENTEST

Americana, SP
2026

Lucas Harteman

FORTALECIMENTO DA SEGURANÇA DA INFORMAÇÃO EM PMES POR MEIO DO PENTEST

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação na área de concentração em Segurança Ofensiva e Pentest.

Orientador(a): Prof. Me. Jonas Bodê

Este trabalho corresponde à versão final do Trabalho de Conclusão de Curso apresentado por Lucas Harteman e orientado pelo(a) Prof. Me. Jonas Bodê

Americana, SP

2026

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi- CEETEPS Dados Internacionais de Catalogação-na-fonte

HARTEMAN, Lucas

Fortalecimento da segurança da informação em pmes por meio do pentest. / Lucas HARTEMAN – Americana, 2026.

54f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Jonas BODÊ

1. Segurança em sistemas de informação. I. HARTEMAN, Lucas II. BODÊ, Jonas III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681.518.5

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Lucas Harteman

FORTALECIMENTO DA SEGURANÇA DA INFORMAÇÃO EM PMES POR MEIO DO PENTEST

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo Centro Paula Souza – Faculdade de Tecnologia de Americana – Ministro Ralph Biasi.
Área de concentração: Segurança Ofensiva

Americana, 09 de junho de 2026

Banca Examinadora:

Jonas Bodê (Presidente)
Mestre
Faculdade de Tecnologia de Americana

Henri Alves de Godoy (Membro)
Doutor
Faculdade de Tecnologia de Americana

Lídia Regina de Carvalho Freitas Barban (Membro)
Especialista
Faculdade de Tecnologia de Americana

AGRADECIMENTOS

Agradeço à minha família, pelo apoio, incentivo e compreensão ao longo de toda a minha trajetória acadêmica. À minha namorada, pelo companheirismo, paciência e apoio constante durante os momentos mais desafiadores desta caminhada. Aos professores, pelos ensinamentos, orientações e contribuições fundamentais para minha formação acadêmica e profissional.

RESUMO

O crescimento exponencial de ataques cibernéticos no Brasil com destaque para pequenas e médias empresas (PMEs) como alvos preferenciais evidencia uma lacuna crítica entre a exposição ao risco e a capacidade de resposta dessas organizações. Este trabalho tem como objetivo investigar como metodologias de Pentest podem ser adaptadas à realidade das PMEs brasileiras como estratégia de fortalecimento da segurança da informação. A pesquisa adota tipologia exploratória com abordagem qualitativa e método de levantamento bibliográfico, baseando-se em normas técnicas da família ISO/IEC 27000, obras acadêmicas consagradas e frameworks reconhecidos pela indústria e pela literatura científica. O referencial teórico aborda os fundamentos da segurança da informação segundo Stallings (2017) e Whitman e Mattord (2022), a origem militar do Red Teaming e sua transição para a cibersegurança, e a diferenciação conceitual entre Vulnerability Assessment, Pentest e Red Team com base no NIST SP 800-115 (2008). São apresentados e detalhados três frameworks metodológicos o Cyber Kill Chain (HUTCHINS; CLOPPERT; AMIN, 2011), o MITRE ATT&CK (STROM et al., 2020) e o PTES (2012) que servem de base para a proposta do modelo. O modelo conceitual desenvolvido estrutura-se em cinco fases adaptadas ao perfil de baixa maturidade das PMEs: planejamento e escopo, reconhecimento, análise de vulnerabilidades, exploração controlada e relatório. O trabalho propõe ainda um arranjo operacional de três camadas Pentester interno, empresa terceirizada de Pentest e Blue Team terceirizado como forma viável e progressiva de elevar a maturidade de segurança da informação nessas organizações. Para validação prática, foi conduzida uma demonstração em laboratório controlado utilizando Kali Linux como máquina atacante e Metasploitable 2 como alvo, com exploração bem-sucedida da CVE-2011-2523 obtendo-se acesso root em menos de cinco minutos com ferramentas gratuitas. Os resultados demonstram que o modelo proposto é tecnicamente fundamentado, financeiramente viável e adaptável às restrições das PMEs brasileiras, servindo como ponto de partida para o desenvolvimento progressivo da maturidade de segurança da informação nessas organizações.

Palavras-chave: Segurança da Informação; Pentest; Segurança Ofensiva; Pequenas e Médias Empresas; Cibersegurança.

ABSTRACT

The exponential growth of cyberattacks in Brazil with small and medium-sized enterprises (SMEs) as preferred targets highlights a critical gap between risk exposure and the response capacity of these organizations. This work aims to investigate how Pentest methodologies can be adapted to the reality of Brazilian SMEs as a strategy for strengthening information security. The research adopts an exploratory typology with a qualitative approach and bibliographic survey method, based on technical standards from the ISO/IEC 27000 family, established academic works, and frameworks recognized by industry and scientific literature. The theoretical framework addresses the fundamentals of information security according to Stallings (2017) and Whitman and Mattord (2022), the military origin of Red Teaming and its transition to cybersecurity, and the conceptual differentiation between Vulnerability Assessment, Pentest, and Red Team based on NIST SP 800-115 (2008). Three methodological frameworks are presented the Cyber Kill Chain, MITRE ATT&CK, and PTES which serve as the basis for the proposed model. The conceptual model is structured in five phases adapted to the low-maturity profile of SMEs. The work also proposes a three-layer operational arrangement as a viable and progressive means of raising the information security maturity of these organizations. For practical validation, a demonstration was conducted in a controlled laboratory environment, successfully exploiting CVE-2011-2523 and obtaining root access in under five minutes using free tools.

Keywords: *Information Security; Pentest; Offensive Security; Small and Medium Enterprises; Cybersecurity.*

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CID	Confidencialidade, Integridade e Disponibilidade
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
EDR	Endpoint Detection and Response
ENISA	European Union Agency for Cybersecurity
ERP	Enterprise Resource Planning
FTP	File Transfer Protocol
GNU	GNU's Not Unix
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBGE	Instituto Brasileiro de Geografia e Estatística
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IP	Internet Protocol
IPS	Intrusion Prevention System
IRC	Internet Relay Chat
ISO	International Organization for Standardization
MITRE	Massachusetts Institute of Technology Research and Engineering
MSSP	Managed Security Service Provider
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSE	Nmap Scripting Engine
OSCP	Offensive Security Certified Professional
OSINT	Open-Source Intelligence
OSSTMM	Open-Source Security Testing Methodology Manual
OWASP	Open Web Application Security Project
PME	Pequena e Média Empresa

PTES	Penetration Testing Execution Standard
SBC	Sociedade Brasileira de Computação
SGSI	Sistema de Gestão de Segurança da Informação
SME	Small and Medium Enterprise
SOC	Security Operations Center
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTP	Tactics, Techniques and Procedures
XSS	Cross-Site Scripting
ZAP	Zed Attack Proxy

SUMÁRIO

1 INTRODUÇÃO

O aumento exponencial de ataques cibernéticos nos últimos anos tem colocado as pequenas e médias empresas como alvos cada vez mais frequentes, apesar de muitas acreditarem que não serão alvo de ataques por não serem foco dos cibercriminosos. Ainda assim, a Kaspersky bloqueou 192 milhões de tentativas de ataques contra PMEs no Brasil em 2023, o equivalente a 365 golpes por minuto (Kaspersky, 2023).

Nesse contexto, as estratégias tradicionais de defesa como antivírus e firewalls, embora fundamentais, podem não ser suficientes para conter ameaças mais sofisticadas. A partir disso, surge a possibilidade de investir em abordagens proativas que permitam antecipar riscos e testar a resiliência das organizações frente a ataques reais, como o *Pentest* (Teste de Penetração), uma abordagem estratégica dentro da segurança ofensiva cujo foco é localizar e expor todas as vulnerabilidades possíveis.

A vulnerabilidade no ambiente cibernético a que empresas de todos os portes estão expostas, associada aos danos que seus dados podem sofrer, é o que leva este estudo a responder à seguinte questão: como a aplicação de Pentest pode ser adaptada à realidade das pequenas e médias empresas como meio eficaz de identificação de vulnerabilidades e fortalecimento da postura de segurança da informação?

O objetivo geral desta pesquisa é investigar como metodologias de Pentest podem ser adaptadas à realidade das pequenas e médias empresas como estratégia de fortalecimento da segurança da informação. Como objetivos específicos, busca-se apresentar os fundamentos teóricos da segurança ofensiva e do Pentest; identificar desafios e limitações na adoção dessas práticas por pequenas empresas; propor um modelo adaptado de aplicação de Pentest baixo custo; identificar benefícios e resultados esperados; e demonstrar, em laboratório controlado, a aplicação prática do modelo.

A relevância do estudo consiste no fato de que empresas de pequeno porte estão inseridas em contexto de transformação digital acelerada, onde riscos cibernéticos aumentam à medida que dependem de sistemas e serviços online. A aplicação de metodologias de Pentest, mesmo de maneira simplificada, pode contribuir para que essas organizações compreendam suas vulnerabilidades e adotem medidas preventivas com baixo investimento.

O trabalho está estruturado em sete capítulos: o segundo apresenta o referencial teórico, o terceiro descreve os materiais e métodos, o quarto propõe o modelo conceitual de Pentest para PMEs, o quinto demonstra a aplicação prática em laboratório controlado, o sexto apresenta os resultados e discussões e o sétimo as considerações finais.

2 REFERENCIAL TEÓRICO

O referencial teórico organiza-se a partir de três pilares fundamentais, os conceitos essenciais de segurança da informação, a evolução histórica do Red Team até sua especialização no Pentest, e os principais frameworks que embasam a proposta prática apresentada. Esta seção busca analisar diferentes perspectivas teóricas, destacando convergências e divergências relevantes, especialmente no contexto das pequenas e médias empresas (PMEs) brasileiras.

2.1 SEGURANÇA DA INFORMAÇÃO

A crescente dependência das organizações em relação aos sistemas digitais tornou a proteção das informações uma estratégia obrigatória. A segurança da informação pode ser compreendida como o conjunto de políticas, controles e mecanismos destinados a preservar três propriedades essenciais dos dados, a confidencialidade, a integridade e a disponibilidade. Essa formulação é feita pela família de normas ISO/IEC 27000, adotada como referência técnica internacional e incorporada ao ordenamento normativo brasileiro pela Associação Brasileira de Normas Técnicas (ABNT).

As normas da família ISO/IEC 27000 fornecem diretrizes amplamente reconhecidas para gestão da segurança da informação, definição de controles e implementação de boas práticas organizacionais. A ISO/IEC 27001:2022 define segurança da informação como a preservação da confidencialidade, integridade e disponibilidade da informação, podendo incluir propriedades adicionais como autenticidade, responsabilização, não repúdio e confiabilidade conforme o contexto organizacional (ABNT, 2022a). Complementarmente, a ISO/IEC 27002:2022 apresenta controles e recomendações voltados à proteção de ativos informacionais, organizando-os em controles organizacionais, de pessoas, físicos e tecnológicos (ABNT, 2022b). Já a ISO/IEC 27032:2023 estabelece diretrizes especificamente voltadas à cibersegurança e à proteção de ambientes digitais conectados.

Na perspectiva acadêmica, Stallings (2017) define a segurança da informação como a proteção de sistemas de informação contra acesso não autorizado, uso indevido, divulgação, interrupção, modificação ou destruição, de modo a garantir a integridade, disponibilidade e confidencialidade dos dados. O autor destaca que esses

princípios devem atuar de forma integrada para assegurar a proteção adequada das informações e dos sistemas organizacionais.

Whitman e Mattord (2022) ampliam essa perspectiva, para os autores, a segurança da informação é um campo multidisciplinar que articula tecnologia, pessoas e processos. Os autores propõem o conceito de *information security management*, que envolve a criação de uma política de segurança, a realização de avaliações de risco e a implementação de controles proporcionais às ameaças identificadas.

> **Confidencialidade:** propriedade que garante que a informação não seja disponibilizada ou divulgada a pessoas, entidades ou processos não autorizados (ABNT, 2022).

> **Integridade:** propriedade que assegura a exatidão e completude da informação, impedindo sua modificação não autorizada (ABNT, 2022).

> **Disponibilidade:** propriedade que garante que a informação e os sistemas estejam acessíveis e utilizáveis quando demandados por usuários e processos autorizados (ABNT, 2022).

2.1.1 Origem Militar do Red Teaming e sua Adaptação para a Cibersegurança

Para compreender o *Red Team* como prática de segurança cibernética, é necessário recuar à sua origem, que antecede o surgimento da internet. O termo nasceu no contexto militar durante a Guerra Fria, designando grupos para simular o comportamento do adversário representado pela cor vermelha, com o objetivo de testar a solidez dos próprios planos e defesas.

Zenko (2015) documenta que a prática foi institucionalizada nos anos 1960 pelo Departamento de Defesa dos Estados Unidos. O autor define o Red Team como um grupo que desempenha o papel de um adversário independente com capacidade de pensar criativamente para identificar fraquezas nos planos, programas, ideias e suposições de uma organização. A essência do método é o pensamento adversarial: não perguntar "o que pode dar certo?", mas "como um inimigo inteligente poderia nos derrotar?".

Conforme discutido por Kennedy et al. (2011), a evolução das práticas de segurança ofensiva e dos testes de intrusão está relacionada à adaptação do pensamento adversarial para o contexto tecnológico. Nesse sentido, a utilização de equipes voltadas à identificação proativa de vulnerabilidades contribuiu para a consolidação do Penetration Testing moderno.

O NIST passou a desenvolver diretrizes técnicas para testes de segurança, resultando na publicação da *Special Publication 800-115* (NIST, 2008), documento que permanece como referência normativa fundamental para a área. Brynielsson et al. (2014) apontam que a adaptação do Red Team para o domínio digital preservou sua característica central, o pensamento de adversário, mas introduziu novas dimensões técnicas relacionadas à exploração de vulnerabilidades em redes, sistemas operacionais e aplicações.

2.1.2 Do Red Team ao Pentest

Embora frequentemente relacionados no contexto da segurança ofensiva, o Red Team e o Pentest possuem escopos, objetivos e metodologias distintas. Enquanto o Pentest busca identificar e validar vulnerabilidades específicas em sistemas, aplicações ou infraestruturas, o Red Team adota uma abordagem mais abrangente, simulando adversários reais em campanhas que combinam técnicas, táticas e procedimentos utilizados por atacantes para avaliar a capacidade de detecção e resposta da organização. O NIST SP 800-115 (2008) estabelece uma classificação clara para as três abordagens de avaliação de segurança, apresentada na tabela 1.

Tabela 1 - Comparativo entre Vulnerability Assessment, Pentest e Red Team

Critério	Aval. Vulnerabilidades	Pentest	Red Team
Objetivo	Identificar falhas	Explorar vulnerabilidades	Simular adversário real
Escopo	Amplo, automatizado	Definido previamente	Aberto, estratégico
Duração	Horas a dias	Dias a semanas	Semanas a meses
Maturidade exigida	Baixa	Moderada	Alta
Viável para PMEs	Alta	Alta (com adaptação)	Baixa a moderada

Fonte: elaborado pelo autor com base em NIST (2008) e Whitman e Mattord (2022).

O Pentest ou teste de penetração avança além da identificação de falhas, seu objetivo é explorar ativamente as vulnerabilidades encontradas, demonstrando o impacto real que um atacante seria capaz de causar.

Kennedy et al. (2011) destacam que exercícios avançados de segurança ofensiva exigem planejamento adequado, definição clara de objetivos e capacidade organizacional para interpretar e responder aos resultados obtidos. Nesse contexto, considera-se que muitas PMEs brasileiras ainda enfrentam dificuldades estruturais e operacionais relacionadas à maturidade em segurança da informação, o que justifica a escolha do Pentest estruturado como abordagem adaptada para esse cenário.

2.1.3 Segurança Ofensiva: fundamentos e abordagens

A segurança ofensiva (*Offensive Security*) compreende um conjunto de abordagens proativas de avaliação e fortalecimento da segurança, baseadas na simulação de técnicas e táticas empregadas por atacantes reais. Diferentemente das abordagens defensivas tradicionais, a segurança ofensiva busca identificar vulnerabilidades por meio da simulação controlada de técnicas utilizadas por atacantes reais, permitindo avaliar falhas antes que elas sejam exploradas de forma maliciosa.

Herzog (2010), no *Open Source Security Testing Methodology Manual* (OSSTMM), descreve essa lógica como a necessidade de testar não apenas o que está protegido, mas como está protegido e se a proteção realmente funciona sob condições adversas. As principais abordagens incluem testes de penetração, exercícios de Red Team, engenharia social e programas de *bug bounty*.

2.1.4 PMEs no contexto brasileiro

As pequenas e médias empresas constituem a espinha dorsal da economia brasileira. De acordo com o IBGE (2022), as empresas de pequeno e médio porte respondem por mais de 98% das unidades produtivas formais do país. Para fins de classificação, o IBGE adota como critério o número de funcionários, microempresas possuem até 9 empregados, pequenas empresas de 10 a 49 no comércio e serviços, ou de 10 a 99 na indústria e médias empresas, de 50 a 249 no comércio e serviços, ou de 100 a 499 na indústria (IBGE, 2022).

As PMEs brasileiras enfrentam uma combinação de fatores de risco, orçamentos de TI reduzidos, ausência de profissionais especializados, uso frequente de softwares sem atualização e baixa maturidade de governança de TI. E essa combinação cria um perfil de vulnerabilidade sistêmica que contrasta com a percepção equivocada de muitos gestores de que suas empresas são alvos de menor interesse para cibercriminosos.

Whitman e Mattord (2022) destacam que a falsa percepção de invisibilidade organizacional pode levar empresas de pequeno porte a negligenciarem práticas essenciais de segurança da informação, aumentando sua exposição a incidentes e ataques cibernéticos.

2.2 FRAMEWORKS E METODOLOGIAS DE SEGURANÇA OFENSIVA

A eficácia de um Pentest depende não apenas das habilidades técnicas do profissional responsável, mas da adoção de uma metodologia estruturada. Esta seção apresenta os três principais *frameworks* que fundamentam a proposta deste trabalho: o *Cyber Kill Chain*, o *MITRE ATT&CK* e o PTES.

2.2.1 Cyber Kill Chain

O modelo *Cyber Kill Chain* foi desenvolvido por Hutchins, Cloppert e Amin (2011) a partir da adaptação do conceito militar de *kill chain* para o domínio da segurança cibernética. O modelo descreve um ataque como uma sequência de sete etapas interdependentes, propondo que a interrupção de qualquer uma delas é suficiente para frustrar o ataque em sua totalidade. As etapas são:

(1) Reconhecimento, coleta de informações sobre o alvo via OSINT e varreduras;

(2) Armamento, desenvolvimento de ferramentas maliciosas;

(3) Entrega, transmissão da carga maliciosa;

(4) Exploração, execução do código malicioso no ambiente alvo;

(5) Instalação, estabelecimento de persistência;

(6) Comando e Controle, canal de comunicação com a infraestrutura do atacante

(7) Ações sobre os objetivos, execução da finalidade última do ataque).

2.2.2 MITRE ATT&CK

O *MITRE ATT&CK* (*Adversarial Tactics, Techniques, and Common Knowledge*) é uma base de conhecimento aberta que documenta táticas, técnicas e procedimentos (TTPs) reais observados em ataques cibernéticos. Desenvolvido pela MITRE Corporation e disponibilizado publicamente desde 2015, é continuamente atualizado com base na análise de incidentes reais.

Strom et al. (2020) descrevem o ATT&CK como uma matriz organizada em múltiplas táticas de alto nível, cada uma associada a diversas técnicas específicas. A matriz Enterprise documenta centenas de técnicas e subtécnicas. Para PMEs, a estrutura do *ATT&CK* permite priorizar técnicas de maior prevalência e impacto, maximizando o valor do teste dentro das restrições orçamentárias disponíveis.

2.2.3 Penetration Testing Execution Standard

O *Penetration Testing Execution Standard* (PTES) é um padrão metodológico desenvolvido por profissionais e pesquisadores da área de segurança ofensiva para

estabelecer uma linguagem comum e boas práticas para a execução de testes de penetração. O PTES organiza o processo de Pentest em sete fases: Pré-engajamento, Coleta de inteligência, Modelagem de ameaças, Análise de vulnerabilidades, Exploração, Pós-exploração e Relatório (PTES, 2012).

Kennedy et al. (2011) destacam a importância da documentação e da elaboração de relatórios no processo de Pentest, uma vez que os resultados obtidos devem ser apresentados de forma clara para apoiar a identificação e correção de vulnerabilidades. Para o contexto das PMEs, o PTES mostra-se especialmente relevante por oferecer uma estrutura adaptável em escopo e complexidade, sem comprometer o rigor metodológico.

3 MATERIAIS E MÉTODOS

Esta pesquisa estrutura-se a partir de quatro dimensões metodológicas complementares, apresentadas a seguir de forma sistematizada.

Quanto à natureza da pesquisa, o trabalho caracteriza-se como pesquisa aplicada, pois tem como finalidade gerar conhecimento com potencial de aplicação prática na solução de um problema específico, a vulnerabilidade cibernética das PMEs brasileiras. Conforme Gil (2002), a pesquisa aplicada “objetiva gerar conhecimentos para aplicação prática, dirigidos à solução de problemas específicos”. O recorte do problema é delimitado ao contexto nacional, considerando as peculiaridades do ambiente regulatório, as pressões impostas pela Lei Geral de Proteção de Dados (LGPD) e o perfil de risco documentado para as PMEs brasileiras.

No que se refere à abordagem da pesquisa, adota-se a abordagem qualitativa. Conforme Minayo (2014), essa abordagem “trabalha com o universo dos significados, dos motivos, das aspirações, das crenças, dos valores e das atitudes”, sendo adequada para a investigação de fenômenos que não se reduzem a métricas quantificadas. No presente estudo, a abordagem qualitativa é pertinente porque o objeto de análise, a adaptação de metodologias de Pentest ao contexto das PMEs, envolve dimensões interpretativas acerca de viabilidade, adequabilidade e praticidade que não seriam capturadas por instrumentos numéricos.

Em relação aos objetivos da pesquisa, o trabalho assume caráter exploratório. Gil (2002) define esse tipo de pesquisa como aquela que “busca maior familiaridade com o problema”, com foco no aprimoramento de conceitos e na descoberta de intuições. A pesquisa exploratória é especialmente adequada quando o tema, embora relevante, ainda apresenta lacunas na literatura quanto à sua operação prática em contextos específicos como o das PMEs brasileiras, nas quais ainda se observam limitações na consolidação de modelos metodológicos de Pentest amplamente difundidos e adaptados à sua realidade operacional.

Quanto aos procedimentos técnicos, a pesquisa combina levantamento bibliográfico e demonstração técnica em laboratório controlado. O levantamento bibliográfico constitui o procedimento principal para a construção do referencial teórico e da proposta conceitual. Conforme Gil (2002), a pesquisa bibliográfica consiste na consulta de material já publicado, incluindo livros, artigos científicos e documentos institucionais. Foram utilizadas como fontes primárias obras acadêmicas como

Stallings (2017), Whitman e Mattord (2022) e Kennedy et al. (2011), normas técnicas da família ISO/IEC 27000, documentos normativos do NIST e os frameworks PTES (2012), MITRE ATT&CK (STROM et al., 2020) e Cyber Kill Chain (HUTCHINS; CLOPPERT; AMIN, 2011). Relatórios de organizações como CERT.br, IBM e ENISA são utilizados exclusivamente para contextualização estatística. A demonstração técnica, apresentada no capítulo 5, configura-se como aplicação prática do modelo em ambiente controlado, sem contato com sistemas reais ou dados de terceiros, e tem por objetivo ilustrar a viabilidade operacional das fases propostas.

A opção pelo laboratório controlado justifica-se por razões éticas e metodológicas: a execução de Pentest em ambientes reais de PMEs sem autorização formal e estrutura contratual adequada configuraria ilicitude nos termos da Lei nº 12.737/2012 (Lei Carolina Dieckmann) e do Código Penal brasileiro. Dessa forma, o laboratório controlado, utilizando Kali Linux como máquina atacante (IP 192.168.10.129) e Metasploitable 2 como alvo (IP 192.168.10.130), em rede virtual isolada configurada no VMware Workstation, representa o procedimento mais adequado para demonstração prática em nível acadêmico.

4 MODELO CONCEITUAL DE PENTEST PARA PMES

Este capítulo apresenta o desenvolvimento central desta pesquisa, um diagnóstico fundamentado do cenário de vulnerabilidades das PMEs brasileiras e, a partir dele, a proposta de um modelo conceitual de Pentest adaptado à realidade dessas organizações. O modelo articula os três frameworks estudados PTES, *MITRE ATT&CK* e *Cyber Kill Chain* e propõe um arranjo operacional viável para PMEs, envolvendo a combinação de um profissional interno, uma empresa terceirizada de Pentest e uma empresa terceirizada de segurança defensiva.

4.1 O CENÁRIO DE VULNERABILIDADE DAS PMES BRASILEIRAS

As vulnerabilidades presentes nas PMEs brasileiras não se limitam apenas a falhas técnicas, envolvendo também questões relacionadas à gestão da segurança da informação, à capacitação dos colaboradores e à ausência de processos organizacionais estruturados. O CERT.br registra anualmente o crescimento de incidentes envolvendo organizações de pequeno porte, com destaque para ataques de *phishing*, varreduras automatizadas e infecções por *ransomware*. A ENISA reforça que PMEs são alvos preferenciais de ataques oportunistas por combinarem presença digital crescente com defesas inadequadas.

4.1.1 Vulnerabilidades técnicas

Stallings (2017) observa que sistemas desatualizados representam a categoria de vulnerabilidade mais explorada por atacantes. Entre as vulnerabilidades técnicas mais prevalentes em PMEs destacam-se a utilização de sistemas sem atualizações regulares, ausência de *firewall* perimetral, uso de senhas fracas ou compartilhadas, ausência de segmentação de rede, e exposição desnecessária de serviços à internet. No modelo *Cyber Kill Chain*, essas vulnerabilidades são identificadas nas fases de Reconhecimento e Exploração, onde um atacante com ferramentas gratuitas é capaz de mapear a superfície de ataque de uma PME típica em minutos.

4.1.2 Vulnerabilidades humanas

Whitman e Mattord (2022) destacam que o fator humano representa um dos principais desafios da segurança da informação, uma vez que falhas de usuários podem comprometer controles técnicos implementados pelas organizações. Nesse sentido, relatórios do CERT.br e da ENISA apontam o phishing como um dos vetores de acesso inicial mais recorrentes em incidentes de segurança. O *MITRE ATT&CK* documenta essas técnicas sob a tática de Acesso Inicial (*Initial Access*), reconhecendo-as como um dos caminhos mais eficazes para a obtenção de acesso não autorizado, por esse motivo, o treinamento contínuo dos funcionários assume papel fundamental.

A conscientização em segurança da informação permite que os colaboradores reconheçam mensagens suspeitas, compreendam os riscos associados ao compartilhamento indevido de informações e adotem práticas mais seguras no uso dos recursos corporativos. Além disso, programas periódicos de capacitação contribuem para a criação de uma cultura organizacional voltada à segurança, reduzindo significativamente a probabilidade de sucesso de ataques baseados em manipulação psicológica.

4.1.3 Vulnerabilidades de processo

Nogueira (2025) destaca que pequenas e médias empresas brasileiras frequentemente enfrentam dificuldades na implementação de práticas adequadas de cibersegurança, especialmente devido a limitações financeiras, escassez de profissionais especializados e baixa priorização estratégica da segurança da informação. Nesse contexto, a norma ISO/IEC 27001:2022 estabelece a política de segurança da informação como elemento fundamental para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI), reconhecendo que controles técnicos e administrativos dependem de diretrizes organizacionais bem definidas (ABNT, 2022). Nesse contexto, considera-se que organizações com baixa maturidade em segurança da informação podem apresentar fragilidades como ausência de rotinas adequadas de backup, inexistência de planos de resposta a incidentes e falhas na gestão de privilégios de acesso.

4.1.4 Perfil de risco da PME brasileira típica e a pertinência do Pentest

A combinação dessas vulnerabilidades evidencia um cenário de risco caracterizado pela presença simultânea de fragilidades técnicas, limitações organizacionais e baixa maturidade em segurança da informação, marcado por organizações com presença digital relevante, sistemas tecnicamente frágeis, colaboradores sem treinamento e ausência de processos formais de segurança.

Whitman e Mattord (2022) destacam que a definição de controles e avaliações de segurança deve considerar o nível de maturidade e a realidade operacional da organização. Nesse sentido, o Pentest pode ser compreendido como um instrumento capaz de auxiliar a organização na identificação prática e priorização de vulnerabilidades e riscos de segurança.

4.2 PROPOSTA DO MODELO CONCEITUAL DE PENTEST PARA PMES

O modelo proposto tem como premissa fundamental a viabilidade, cinco objetivos centrais guiam sua construção: (1) definir o escopo, os objetivos e as autorizações da avaliação; (2) identificar ativos e possíveis superfícies de ataque; (3) localizar e classificar vulnerabilidades existentes; (4) validar, de forma controlada, o impacto e a exploração das vulnerabilidades identificadas; e (5) documentar os resultados obtidos e propor ações de mitigação e melhoria da segurança.

Tabela 2 - Visão geral das fases do modelo conceitual de Pentest para PMEs

Fase	Etapa	Objetivo	Referência metodológica
1	Planejamento e escopo	Definir objetivos e autorizações	PTES: Pré-engajamento; NIST SP 800-115
2	Reconhecimento	Identificar ativos e superfície de ataque	PTES: Intelligence Gathering; MITRE ATT&CK
3	Análise de vulnerabilidades	Localizar e classificar falhas (CVSS)	PTES: Vulnerability Analysis; CVSS
4	Exploração controlada	Validar risco real das vulnerabilidades	PTES: Exploitation; Cyber Kill Chain; MITRE ATT&CK
5	Relatório de vulnerabilidades	Documentar resultados e propor melhorias	PTES: Reporting; NIST SP 800-115

Fonte: elaborado pelo autor com base em PTES (2012), NIST (2008) e MITRE Corporation (2020).

4.2.1 Fase 1: Planejamento e escopo

A fase de planejamento e escopo estabelece os limites, objetivos e condições sob os quais o Pentest será executado. Nessa etapa são definidos os ativos que serão avaliados, as técnicas permitidas, as restrições operacionais, os responsáveis envolvidos e as autorizações necessárias para a realização dos testes. O PTES (2012) denomina esta etapa de Pré-engajamento e a posiciona como a fundação sobre a qual todas as demais fases se sustentam.

No contexto das PMEs, o interlocutor é frequentemente o próprio proprietário da empresa ou um gerente sem formação técnica, o que exige comunicação clara e foco nos impactos para o negócio. Além disso, o NIST SP 800-115 (2008) ressalta que a formalização do escopo e das autorizações é indispensável, pois a execução de testes sem consentimento explícito pode ser caracterizada como acesso não autorizado, independentemente das intenções do profissional responsável.

4.2.2 Fase 2: Reconhecimento e coleta de informações

A fase de reconhecimento mapeia a superfície de ataque antes de qualquer interação direta com os sistemas. A técnica de OSINT (*Open Source Intelligence*) permite construir um mapa detalhado da infraestrutura tecnológica de uma organização sem jamais tocar em seus sistemas, por meio de registros de domínio, certificados SSL expostos, perfis em redes sociais e metadados de documentos públicos, situação frequentemente observada em PMEs que não possuem processos estruturados de proteção e gerenciamento de informações. O *MITRE ATT&CK* documenta essas técnicas sob a tática de Reconhecimento (T1595, T1590, T1593).

Além da identificação de hosts e serviços expostos, a fase de reconhecimento permite compreender a superfície de ataque da organização, reunindo informações que servirão de base para as etapas subsequentes do Pentest. Dados como versões de software, portas abertas, domínios associados, certificados digitais e tecnologias utilizadas podem revelar potenciais vetores de ataque antes mesmo da realização de testes mais invasivos. Para as PMEs, essa etapa possui importância especial, pois muitas vulnerabilidades decorrem de falhas de configuração, serviços desnecessariamente expostos à Internet ou ativos que não são devidamente monitorados pela equipe de TI.

4.2.3 Fase 3: Análise de vulnerabilidades

A análise de vulnerabilidades consiste na identificação e avaliação sistemática de falhas de segurança que possam comprometer a confidencialidade, integridade ou disponibilidade dos ativos organizacionais. Essa atividade deve combinar ferramentas automatizadas de varredura com verificações manuais, aumentando a precisão dos resultados e reduzindo a ocorrência de falsos positivos.

Após a coleta das evidências, as vulnerabilidades identificadas devem ser classificadas de acordo com seu nível de risco. Para essa finalidade, recomenda-se a utilização do CVSS (Common Vulnerability Scoring System), que estabelece uma escala padronizada de 0 a 10 baseada em fatores como impacto potencial e facilidade de exploração. Em ambientes de PMEs, essa abordagem favorece a alocação eficiente de recursos, permitindo que as ações corretivas sejam direcionadas prioritariamente às vulnerabilidades mais críticas.

4.2.4 Fase 4: Exploração controlada

A exploração controlada representa a etapa em que as vulnerabilidades identificadas são submetidas a testes práticos para comprovar sua explorabilidade e mensurar seu impacto real. O objetivo não é causar danos ao ambiente, mas sim demonstrar de forma segura e controlada como um agente malicioso poderia explorar determinada falha. Para isso, todas as ações devem ser previamente autorizadas, monitoradas e registradas.

A seleção das técnicas de exploração pode ser orientada pelo framework MITRE ATT&CK, que cataloga TTPs (Táticas, Técnicas e Procedimentos) observadas em ataques reais. No contexto das PMEs, destacam-se técnicas relacionadas à exploração de credenciais fracas (T1110 – Brute Force), comprometimento de aplicações expostas à Internet (T1190 – Exploit Public-Facing Application) e elevação de privilégios após o acesso inicial. A validação dessas vulnerabilidades permite determinar com maior precisão o risco efetivo ao negócio e subsidiar a definição de medidas corretivas prioritárias.

4.2.5 Fase 5: Relatório de vulnerabilidades

Kennedy et al. (2011) destacam a importância da documentação e da comunicação dos resultados obtidos durante o processo de Pentest. O modelo proposto divide-se em duas seções, o sumário executivo para gestores focado nos riscos de negócio e seção técnica detalhada para a equipe de correção, com pontuação CVSS, referências ao *MITRE ATT&CK* e recomendações priorizadas. O relatório é o elo central do arranjo operacional: é a partir dele que a segurança defensiva terceirizada compreende o que precisa ser corrigido e em qual ordem.

Para as PMEs, a efetividade do relatório depende não apenas da qualidade técnica das descobertas, mas também da forma como elas são comunicadas. Considerando que muitas dessas organizações não dispõem de equipes dedicadas à segurança da informação, torna-se essencial que os resultados sejam apresentados de maneira objetiva e compreensível. A inclusão de descrições simplificadas das vulnerabilidades, exemplos dos possíveis impactos e recomendações de correção passo a passo contribui para reduzir barreiras técnicas e facilitar a implementação das melhorias propostas. Dessa forma, o relatório deixa de ser apenas um documento técnico e passa a atuar como instrumento de orientação para o fortalecimento gradual da postura de segurança da organização.

4.3 FERRAMENTAS ACESSÍVEIS PARA PMES

A viabilidade financeira do modelo proposto depende diretamente da disponibilidade de ferramentas de qualidade profissional sem custos de licenciamento. Diferentemente de grandes organizações, que frequentemente dispõem de orçamentos específicos para aquisição de soluções comerciais de segurança, as PMEs geralmente precisam equilibrar investimentos em cibersegurança com outras demandas operacionais consideradas prioritárias. Essa limitação orçamentária faz com que a adoção de ferramentas gratuitas ou de código aberto represente uma alternativa estratégica para fortalecer a segurança da informação sem comprometer a sustentabilidade financeira do negócio.

4.3.1 Nmap (Network Mapper)

O Nmap é a ferramenta de mapeamento de redes mais amplamente utilizada do mundo. Sua função principal é a identificação de hosts ativos, portas abertas, serviços em execução e versões de software, a ferramenta é um importante recurso para as etapas de reconhecimento e enumeração em avaliações de segurança, sua principal limitação no contexto de PMEs é a necessidade de interpretação qualificada dos resultados.

4.3.2 OpenVAS

O OpenVAS é um scanner de vulnerabilidades de código aberto mantido pela Greenbone Networks, capaz de identificar automaticamente vulnerabilidades conhecidas com referências a CVEs. Sua principal limitação é a taxa de falsos positivos, dessa forma, os resultados devem ser sempre validados manualmente antes de serem incluídos no relatório final.

4.3.3 OWASP ZAP

O OWASP ZAP (Zed Attack Proxy) é uma ferramenta de código aberto desenvolvida pela OWASP para identificação de vulnerabilidades em aplicações web. A ferramenta atua como um proxy intermediário entre o navegador e a aplicação, permitindo a inspeção do tráfego HTTP e HTTPS, bem como a realização de testes automatizados e manuais de segurança.

Entre seus principais recursos destacam-se a detecção de vulnerabilidades como Cross-Site Scripting (XSS), falhas de configuração de segurança, exposição inadequada de informações e outros problemas frequentemente encontrados em aplicações web. Além disso, o OWASP ZAP oferece funcionalidades de varredura automatizada, mapeamento de aplicações e análise de requisições e respostas, tornando-se uma alternativa acessível para organizações com recursos limitados.

No modelo proposto, o OWASP ZAP pode ser empregado durante as fases de reconhecimento e análise de vulnerabilidades, auxiliando na identificação de falhas em aplicações web expostas à Internet. Por ser uma ferramenta gratuita e

amplamente adotada pela comunidade de segurança, sua utilização contribui para a viabilidade da aplicação de práticas de Pentest em PMEs.

4.3.4 Metasploit Framework (Community Edition)

O Metasploit Framework é o *framework* de exploração de vulnerabilidades mais utilizado na área. O Metasploit Framework é uma das principais ferramentas utilizadas em testes de penetração, especialmente em atividades relacionadas à validação prática de vulnerabilidades.

4.3.5 Wireshark

O Wireshark é o analisador de protocolos de rede mais utilizado do mundo, capaz de capturar e inspecionar o tráfego em tempo real. É especialmente útil para identificar o uso de protocolos legados inseguros como Telnet, FTP e HTTP sem TLS.

Tabela 3 - Ferramentas acessíveis para PMEs

Ferramenta	Função principal	Fase do modelo	Limitação principal	Custo
Nmap	Scanner de rede e serviços	Reconhecimento e Análise	Requer interpretação qualificada	Gratuito
OpenVAS	Scanner de vulnerabilidades	Análise de Vulnerabilidades	Alta taxa de falsos positivos	Gratuito
OWASP ZAP	Testes em aplicações web	Análise e Exploração (web)	Escopo restrito a apps web	Gratuito
Wireshark	Análise de tráfego de rede	Reconhecimento e Análise	Requer conhecimento em redes	Gratuito
Metasploit	Framework de exploração	Exploração Controlada	Risco se mal configurado	Gratuito

Fonte: elaborado pelo autor com base em Kennedy et al. (2011) e PTES (2012).

4.4 INTEGRAÇÃO DOS FRAMEWORKS NO MODELO PROPOSTO

O PTES funciona como a estrutura metodológica central do modelo, definindo as fases operacionais do processo de Pentest, os procedimentos adotados e os padrões de documentação. O MITRE ATT&CK complementa essa estrutura ao fornecer uma base de conhecimento das técnicas e táticas utilizadas em ataques reais, permitindo alinhar os testes executados aos comportamentos observados em ameaças contemporâneas. Por sua vez, o Cyber Kill Chain contribui com uma visão sequencial das etapas percorridas pelos atacantes durante uma invasão, possibilitando relacionar as vulnerabilidades identificadas aos diferentes momentos do ciclo de comprometimento e evidenciar pontos em que mecanismos defensivos podem detectar, interromper ou mitigar o ataque.

4.5 VIABILIDADE DO MODELO: O ARRANJO OPERACIONAL PARA PMES

A adoção de práticas de Pentest em PMEs enfrenta desafios relacionados à limitação de recursos financeiros, à escassez de profissionais especializados e à necessidade de manter atividades de segurança de forma contínua. Para tornar o modelo proposto compatível com essa realidade, esta pesquisa apresenta um arranjo operacional composto por três camadas complementares, responsáveis pela identificação, validação e mitigação de vulnerabilidades ao longo do tempo.

4.5.1 Camada 1: O Pentester interno

A primeira camada é composta por um profissional interno em formação, preferencialmente um estagiário ou analista júnior de TI com o foco dos estudos em segurança ofensiva, responsável pelas atividades de reconhecimento, monitoramento e identificação inicial de vulnerabilidades. Considerando a realidade financeira das PMEs, a contratação de especialistas dedicados em segurança ofensiva nem sempre é viável. Dessa forma, o modelo propõe a capacitação gradual de profissionais em início de carreira para executar tarefas operacionais apoiadas por ferramentas automatizadas e procedimentos padronizados.

Além dos benefícios para a organização, essa abordagem contribui para o desenvolvimento profissional do colaborador. O mercado de segurança ofensiva

frequentemente exige experiência prévia mesmo para vagas de entrada, criando uma barreira para profissionais que desejam ingressar na área. Ao participar das atividades de reconhecimento, análise de vulnerabilidades e monitoramento, o profissional adquire experiência prática em um ambiente real, desenvolvendo competências que dificilmente seriam obtidas apenas por meio de cursos ou laboratórios acadêmicos. Dessa forma, o modelo gera benefícios mútuos, a empresa desenvolve capacidades internas de segurança a baixo custo, enquanto o colaborador obtém experiência relevante para sua evolução na área de cibersegurança.

4.5.2 Camada 2: A empresa terceirizada de Pentest

A contratação de uma empresa especializada em Pentest permite que a organização obtenha uma avaliação independente de sua postura de segurança, reduzindo possíveis vieses associados às avaliações realizadas exclusivamente por equipes internas. Além da validação técnica das vulnerabilidades identificadas durante as etapas de reconhecimento e análise, a empresa contratada contribui com a experiência acumulada em diferentes ambientes organizacionais e setores de mercado, ampliando a capacidade de identificação de riscos relevantes.

Entre as principais atividades executadas por essas empresas destacam-se a realização de testes de invasão em aplicações web, infraestrutura de rede, ambientes internos e serviços expostos à internet, bem como a validação prática de vulnerabilidades identificadas por ferramentas automatizadas. Diferentemente dos scanners de vulnerabilidades, que podem gerar falsos positivos, o Pentest busca comprovar a exploração real das falhas encontradas.

Outro benefício importante está relacionado à qualidade da documentação produzida. Empresas especializadas normalmente entregam relatórios estruturados contendo descrição das vulnerabilidades identificadas, evidências técnicas, classificação de criticidade baseada em padrões reconhecidos, como o CVSS, e recomendações de mitigação priorizadas. Esses relatórios auxiliam gestores na tomada de decisão e servem como referência para as atividades executadas posteriormente pela equipe interna ou pela empresa terceirizada de Segurança Defensiva.

Além disso, o mercado brasileiro oferece empresas especializadas com modelos de contratação escalonáveis, permitindo que PMEs realizem avaliações

periódicas sem a necessidade de manter profissionais altamente especializados em regime permanente. Dessa forma, a contratação pontual de serviços de Pentest representa uma alternativa economicamente mais acessível para organizações que desejam validar sua segurança de forma profissional, mantendo compatibilidade com suas limitações orçamentárias.

Deste modo, a periodicidade da contratação deve ser definida de acordo com o porte da organização, a criticidade dos ativos e a frequência de mudanças em sua infraestrutura tecnológica. Para a realidade da maioria das PMEs, recomenda-se a realização de Pentests completos pelo menos uma vez por ano, bem como após alterações significativas em sistemas, aplicações ou na arquitetura de rede. Essa abordagem permite identificar novas vulnerabilidades introduzidas por mudanças no ambiente e acompanhar a evolução da postura de segurança ao longo do tempo.

4.5.3 Camada 3: A empresa terceirizada de segurança defensiva

A terceira camada é uma empresa de segurança defensiva terceirizada ou MSSP (*Managed Security Service Provider*) responsável por implementar as correções recomendadas no relatório do Pentest e manter os controles defensivos ao longo do tempo. Herzog (2010) enfatiza que a identificação de vulnerabilidades deve estar associada à implementação contínua de medidas corretivas e processos de melhoria da segurança. Nesse contexto, modelos terceirizados de segurança, como MSSPs, podem representar uma alternativa viável para PMEs que possuem limitações técnicas ou operacionais para manter equipes internas especializadas.

No contexto das PMEs, a atuação da empresa terceirizada de segurança defensiva não exige necessariamente a implementação de estruturas complexas, como Centros de Operações de Segurança (SOC) dedicados. O foco principal consiste na manutenção contínua dos controles de segurança recomendados pelo Pentest, garantindo que as vulnerabilidades identificadas sejam efetivamente corrigidas e monitoradas ao longo do tempo.

Entre os serviços mais relevantes para esse cenário destacam-se a gestão de atualizações e correções de segurança (*patch management*), administração de firewalls, monitoramento de eventos e logs, gerenciamento de backups e suporte na resposta a incidentes. Essas atividades contribuem para reduzir a superfície de ataque

e aumentar a capacidade de recuperação da organização diante de falhas ou ataques cibernéticos.

Uma alternativa acessível para PMEs é a adoção de soluções de segurança baseadas em assinatura. Como exemplo, o Microsoft Defender for Business oferece recursos de proteção avançada para endpoints, detecção e resposta a ameaças (EDR), gerenciamento de vulnerabilidades, monitoramento de dispositivos e resposta automatizada a incidentes. Esse modelo permite que pequenas e médias empresas tenham acesso a funcionalidades tradicionalmente disponíveis apenas em soluções corporativas de maior porte, sem a necessidade de manter equipes especializadas dedicadas exclusivamente à segurança da informação.

A disponibilidade de serviços gerenciados de segurança e soluções comerciais voltadas ao segmento de PMEs reforça a viabilidade financeira do modelo proposto. Em vez de realizar elevados investimentos iniciais em infraestrutura e pessoal especializado, as organizações podem adotar uma abordagem gradual baseada em ferramentas gratuitas, profissionais internos em desenvolvimento e serviços terceirizados escaláveis, compatibilizando a evolução da maturidade em segurança com sua realidade orçamentária.

4.6 Modelo integrado da proposta

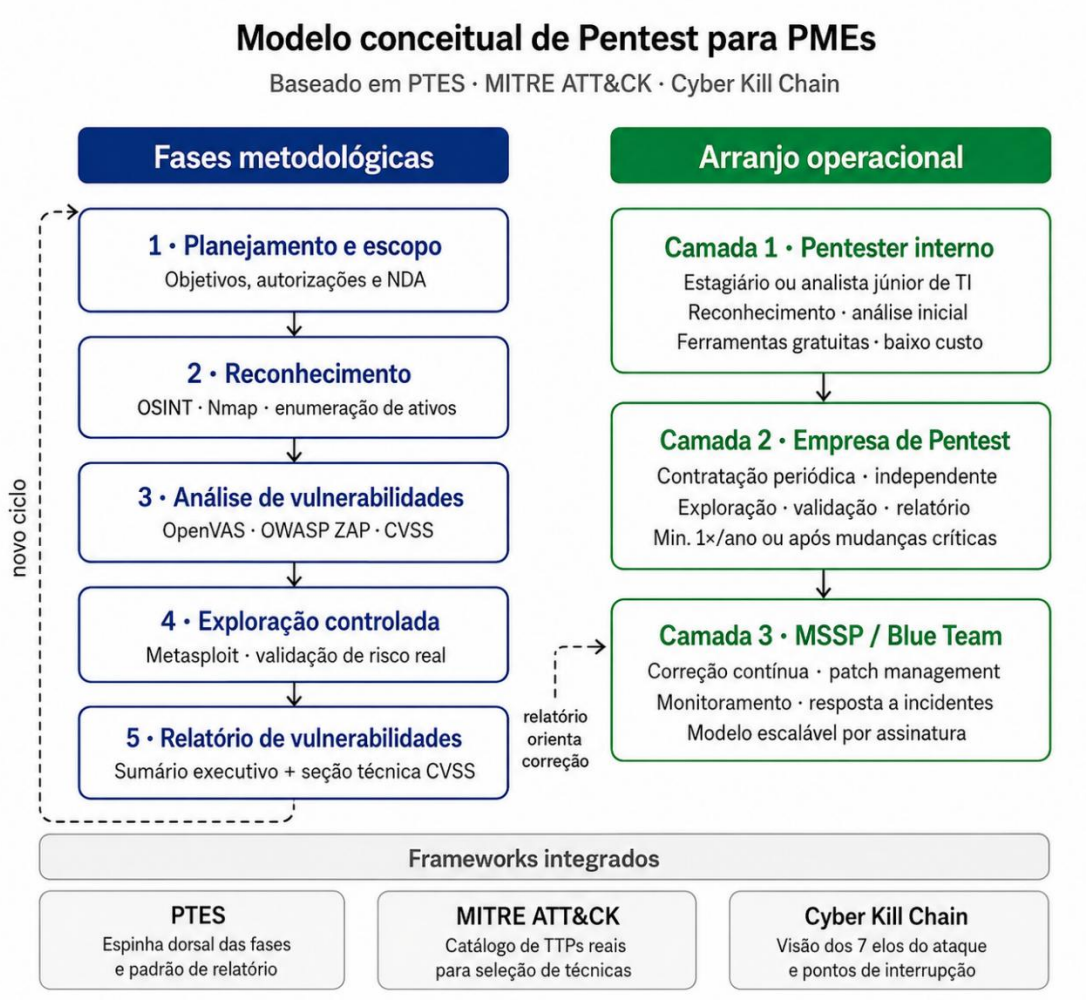
Nenhuma das três camadas propostas é suficiente isoladamente para atender às necessidades de segurança das pequenas e médias empresas. Organizações desse porte frequentemente enfrentam limitações relacionadas à disponibilidade de recursos financeiros, ausência de equipes especializadas, restrições operacionais e baixo nível de maturidade em segurança da informação. Além disso, muitas PMEs ainda concentram seus investimentos em aspectos operacionais do negócio, tratando a segurança cibernética de forma reativa ou secundária. Nesse cenário, a implementação de práticas avançadas de segurança ofensiva exige abordagens flexíveis e adaptáveis, capazes de equilibrar rigor metodológico, viabilidade operacional e compatibilidade com a realidade estrutural dessas organizações.

Dessa forma, o modelo desenvolvido neste trabalho busca integrar diferentes abordagens de segurança ofensiva em uma estrutura única e complementar. A proposta combina o PTES como base metodológica para organização das etapas do Pentest, o MITRE ATT&CK como referência prática das técnicas ofensivas utilizadas

em ataques reais e o Cyber Kill Chain como modelo sequencial das fases de comprometimento percorridas pelos atacantes. A integração desses frameworks permite estruturar o processo de avaliação de segurança de maneira mais consistente, relacionando metodologias de execução, comportamentos ofensivos observados em cenários reais e as diferentes etapas do ciclo de ataque.

A Figura 1 apresenta a organização integrada do modelo proposto, relacionando as fases operacionais do Pentest, os frameworks utilizados como suporte conceitual e o arranjo operacional em camadas.

Figura 1 - Modelo integrado para Pentest



Fonte: Elaborado pelo autor (2026).

5 DEMONSTRAÇÃO PRÁTICA EM AMBIENTE CONTROLADO

Este capítulo apresenta a aplicação prática do modelo conceitual proposto, por meio de uma demonstração executada em laboratório controlado. O objetivo é ilustrar as fases de reconhecimento, enumeração e exploração com ferramentas de código aberto. Todos os testes foram conduzidos em ambiente isolado, sem qualquer interação com sistemas reais ou dados de terceiros.

5.1 CONFIGURAÇÃO DO AMBIENTE DE LABORATÓRIO

O laboratório foi configurado com o VMware Workstation como plataforma de virtualização, em rede virtual isolada (modo *Host-Only*), composto pelas máquinas apresentadas na tabela 4.

Tabela 4 - Configuração do ambiente de laboratório

Máquina	Sistema operacional	Endereço IP	Papel no laboratório
Máquina atacante	Kali Linux	192.168.10.129	Execução das ferramentas
Máquina alvo	Metasploitable 2	192.168.10.130	Sistema intencionalmente vulnerável

Fonte: elaborado pelo autor (2026).

O Kali Linux é uma distribuição GNU/Linux desenvolvida pela Offensive Security, amplamente utilizada em atividades de testes de penetração e segurança ofensiva. A distribuição sucedeu ao BackTrack Linux e consolidou-se como uma das principais plataformas voltadas à execução de ferramentas de Pentest.

O Metasploitable 2 é uma máquina virtual desenvolvida pela Rapid7, intencionalmente configurada com serviços vulneráveis e senhas fracas, simulando o perfil de uma organização com baixa maturidade de segurança.

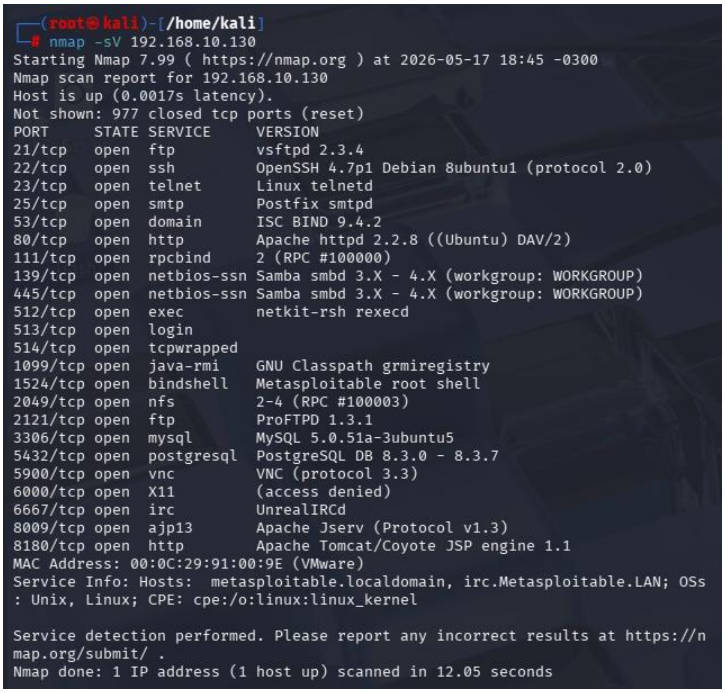
5.2 FASE DE RECONHECIMENTO E ENUMERAÇÃO COM NMAP

O Nmap foi utilizado em dois comandos complementares, correspondentes à Fase 2 do modelo e à tática de Reconhecimento do *MITRE ATT&CK* (STROM et al., 2020).

5.2.1 Enumeração de serviços e versões

O primeiro comando executado foi: Nmap -sV 192.168.10.130 o parâmetro **-sV** instrui o Nmap a realizar a detecção de versões de serviço (*service version detection*), além de identificar quais portas estão abertas, a ferramenta envia sondas específicas para determinar qual serviço está em execução e qual sua versão exata. Essa informação é fundamental pois versões específicas frequentemente estão associadas a vulnerabilidades catalogadas no CVE.

Figura 2 - Resultado do comando nmap -sV 192.168.10.130



Fonte: captura de tela obtida pelo autor durante a demonstração (2026).

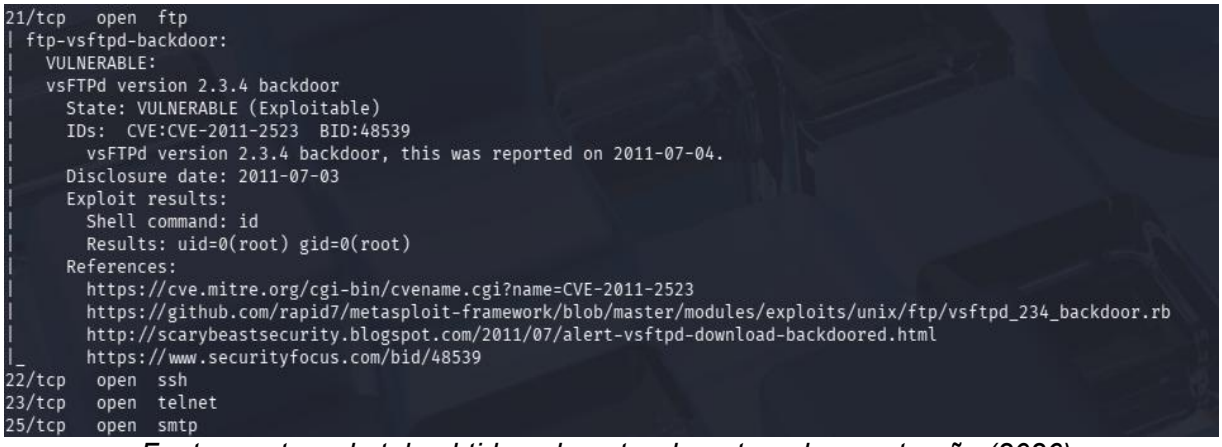
O resultado, apresentado na Figura 2, revela 23 portas abertas com serviços que incluem FTP (portas 21 e 2121), SSH (porta 22), Telnet (porta 23), HTTP (portas 80 e 8180), MySQL (porta 3306), PostgreSQL (porta 5432) e IRC (porta 6667). Para os fins desta demonstração, o foco recai sobre a porta 21 (FTP), na qual foi

identificado o serviço **vsftpd 2.3.4,** versão conhecida por conter um *backdoor* malicioso inserido em seu código-fonte.

5.2.2 Identificação de vulnerabilidades com NSE

O segundo comando executado foi: Nmap –script vuln 192.168.10.130, o parâmetro **--script vuln** ativa o *Nmap Scripting Engine* (NSE) com a categoria de scripts de vulnerabilidades. O NSE executa scripts Lua que correlacionam os serviços identificados com registros de CVEs e bases de dados de exploits. Embora não substitua scanners especializados, como o OpenVAS, esse recurso permite ao Nmap realizar verificações preliminares de vulnerabilidades conhecidas e apoiar a fase de análise de segurança.

Figura 3 - Resultado do comando nmap --script vuln



Fonte: captura de tela obtida pelo autor durante a demonstração (2026).

O resultado, apresentado na Figura 3, confirma a presença do *backdoor* no serviço FTP da porta 21 com estado *VULNERABLE* (*Exploitable*). A tabela 5 apresenta as informações identificadas pela varredura.

Tabela 5 - Dados da CVE-2011-2523 identificados pela varredura NSE

Campo	Informação identificada
Vulnerabilidade	vsFTPd versão 2.3.4 backdoor
Estado	**VULNERABLE (Exploitable)**
CVE	CVE-2011-2523 / BID:48539
Data de divulgação	2011-07-03
Resultado do exploit	**uid=0(root) gid=0(root) acesso root confirmado**

Fonte: elaborado pelo autor com base nos resultados da varredura (2026).

O CVE-2011-2523 documenta um dos casos mais notórios de comprometimento da cadeia de suprimentos de software, em 2011 o código-fonte do vsftpd 2.3.4 foi substituído por uma versão maliciosa contendo um *backdoor* que abria um shell com privilégios de root na porta 6200/TCP. O incidente representa o risco da ausência de verificação de integridade de pacotes de software.

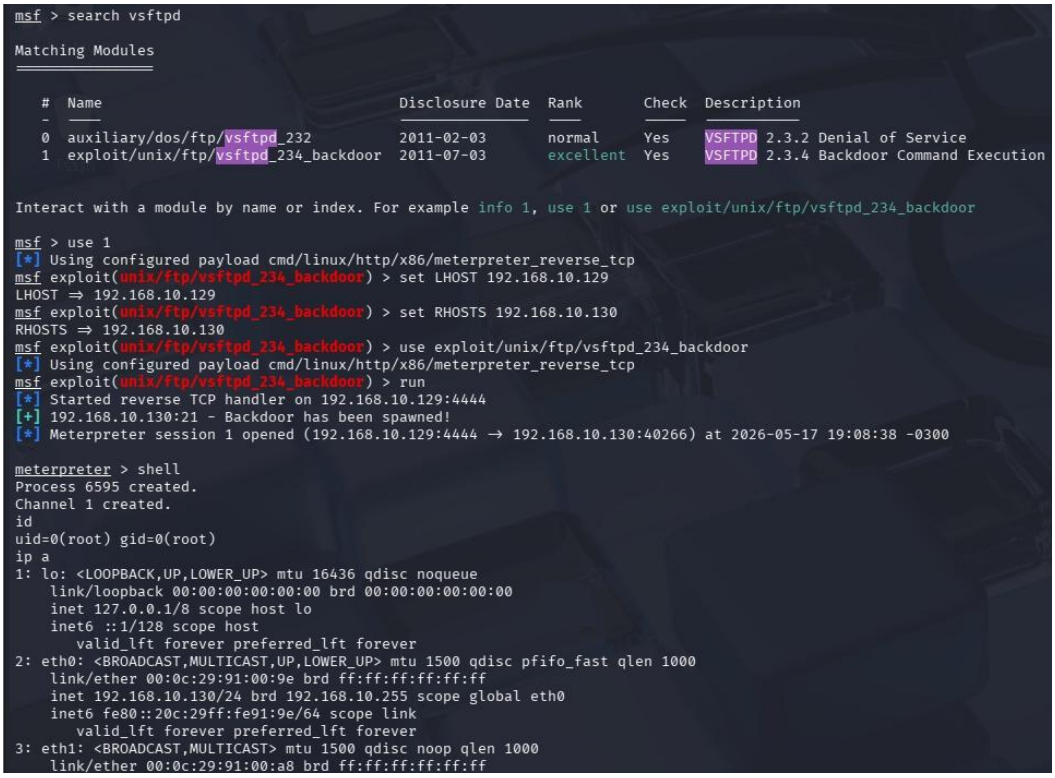
5.3 FASE DE EXPLORAÇÃO CONTROLADA COM METASPLOIT FRAMEWORK

Com a vulnerabilidade CVE-2011-2523 confirmada durante a etapa de enumeração, a fase de exploração controlada foi conduzida por meio do módulo exploit/unix/ftp/vsftpd_234_backdoor do Metasploit Framework. Esse módulo explora uma backdoor inserida maliciosamente na versão 2.3.4 do serviço VSFTPD, vulnerabilidade amplamente documentada e associada à execução remota de comandos sem autenticação prévia. A utilização do módulo permitiu automatizar o processo de exploração, simulando um cenário real de comprometimento inicial em ambientes com serviços desatualizados e expostos à rede.

Durante o procedimento, foram configurados os parâmetros básicos do exploit, incluindo o endereço IP do alvo e a porta utilizada pelo serviço FTP vulnerável. Após a execução do módulo, foi estabelecida uma sessão remota no sistema comprometido, demonstrando que a exploração poderia ser realizada com baixo nível de complexidade técnica e utilizando ferramentas amplamente disponíveis na comunidade de segurança ofensiva. Esse resultado evidencia como vulnerabilidades

conhecidas e não corrigidas podem permitir comprometimento completo do sistema mesmo sem técnicas avançadas de ataque.

Figura 4 - Exploração da CVE-2011-2523 via Metasploit.



Fonte: captura de tela obtida pelo autor durante a demonstração (2026).

A Figura 4 documenta a exploração completa. O módulo foi classificado pelo Metasploit com *rank* excelente**,** a classificação mais alta de confiabilidade. Em menos de dois segundos, a sessão Meterpreter foi estabelecida: “Meterpreter session 1 opened (192.168.10.129:4444 - 192.168.10.130:40266)” ou seja, a máquina atacante se conectou com a máquina alvo. O comando “id” retornou “uid=0(root) gid=0(root)” acesso com privilégios máximos obtido sem qualquer etapa adicional de escalada.

5.3.1 Mapeamento na Cyber Kill Chain e MITRE ATT&CK

A tabela 6 apresenta o mapeamento de cada etapa da exploração na *Cyber Kill Chain* e no *MITRE ATT&CK*.

Tabela 6 - Mapeamento da exploração na Cyber Kill Chain e MITRE ATT&CK

Elo da Kill Chain	Ação realizada	Técnica MITRE ATT&CK
1. Reconhecimento	nmap -sV: identificação do vsftpd 2.3.4	T1595: Active Scanning
2. Armamento	Seleção do módulo exploit no Metasploit	T1587: Develop Capabilities
3. Entrega	Requisição FTP com backdoor trigger	T1190 : Exploit Public-Facing Application
4. Exploração	Ativação do backdoor, abertura porta 6200	T1190 : Exploit Public-Facing Application
5. Instalação	Sessão Meterpreter estabelecida	T1543: Create or Modify System Process
6. Comando e Controle	Canal reverso TCP 192.168.10.129:4444	T1571: Non-Standard Port
7. Ações/Objetivos	Shell root obtido; acesso total ao sistema	T1078: Valid Accounts (root)

Fonte: elaborado pelo autor com base em Hutchins, Cloppert e Amin (2011) e MITRE ATT&CK (STROM et al., 2020).

A demonstração percorreu todos os sete elos da *Cyber Kill Chain* em menos de cinco minutos, a partir de um único serviço desatualizado. Isso reforça a proposta de Hutchins, Cloppert e Amin (2011) de que diferentes etapas do ciclo de ataque podem ser utilizadas para identificação, contenção ou interrupção de atividades maliciosas. No caso da PME simulada, não foram identificados mecanismos de defesa capazes de interromper o ataque ao longo das etapas analisadas.

5.4 IMPACTOS IDENTIFICADOS E RECOMENDAÇÕES DE MITIGAÇÃO

O comprometimento total do sistema, com ferramentas gratuitas e técnica documentada há mais de uma década evidencia impactos que, em ambiente real de PME, seriam potencialmente devastadores, com o comprometimento total do sistema, risco de movimentação lateral em redes sem segmentação e possibilidade de *ransomware* ou exfiltração de dados. A tabela 7 apresenta as recomendações de mitigação priorizadas.

Tabela 7 - Recomendações de mitigação priorizadas

#	Vulnerabilidade	Recomendação	Criticidade (CVSS)	Custo
1	vsftpd 2.3.4 (CVE-2011-2523)	Atualizar imediatamente ou desativar o FTP	**Crítica (10.0)**	Baixo
2	23 portas e serviços expostos	Desativar serviços não utilizados; implementar firewall	Alta	Baixo
3	Telnet em texto claro (porta 23)	Substituir Telnet por SSH; desativar Telnet	Alta	Baixo
4	Ausência de IDS/IPS	Implementar Snort ou Suricata (código aberto)	Média	Baixo
5	Ausência de gestão de patches	Implementar processo formal de atualização periódica	Alta	Baixo

Fonte: elaborado pelo autor com base nos resultados da demonstração e no NIST SP 800-115 (2008).

5.5 O QUE A DEMONSTRAÇÃO EVIDENCIA SOBRE AS PMES

A demonstração evidencia que a CVE-2011-2523, divulgada em 2011 há mais de 14 anos, ainda poderia ser explorada em ambientes sem processos adequados de gestão de vulnerabilidades e atualização de sistemas. Segundo Stallings (2017), a manutenção inadequada e a permanência de vulnerabilidades conhecidas representam fatores relevantes para o comprometimento de ambientes corporativos. No cenário demonstrado, a simples atualização ou desativação do serviço vulnerável teria sido suficiente para eliminar completamente o vetor de ataque utilizado.

Além de ilustrar os riscos associados à manutenção de serviços vulneráveis, a demonstração permitiu validar aspectos centrais do modelo proposto nesta pesquisa. Primeiramente, confirmou a eficácia da fase de reconhecimento na identificação de serviços expostos e potenciais vulnerabilidades por meio de ferramentas gratuitas e amplamente acessíveis. Em seguida, evidenciou a importância da análise e da exploração controlada para comprovar o impacto real das falhas identificadas, reduzindo a dependência exclusiva de resultados automatizados e permitindo uma avaliação mais precisa dos riscos.

Os resultados obtidos também reforçam a relevância da documentação produzida durante o processo de Pentest. A apresentação de evidências concretas, como a identificação da vulnerabilidade, a validação da exploração e a obtenção de acesso privilegiado, contribui para tornar os riscos mais compreensíveis para gestores não técnicos, facilitando a priorização de investimentos e ações corretivas.

Por fim, a demonstração reforça a necessidade de um processo contínuo de correção e monitoramento das vulnerabilidades identificadas. A simples descoberta de falhas não produz benefícios efetivos sem a implementação das medidas recomendadas. Nesse contexto, a inclusão de uma empresa terceirizada de Segurança Defensiva no arranjo operacional proposto mostra-se fundamental para garantir a aplicação das correções, a manutenção dos controles de segurança e o acompanhamento permanente da postura de segurança da organização.

6 RESULTADOS E DISCUSSÕES

Os resultados obtidos ao longo desta pesquisa permitiram avaliar a viabilidade da aplicação de práticas de Pentest em pequenas e médias empresas por meio de um modelo simplificado e adaptado à sua realidade operacional. A análise da literatura demonstrou que as PMEs estão frequentemente expostas a vulnerabilidades técnicas, humanas e processuais, muitas vezes sem possuir recursos suficientes para manter equipes especializadas ou investir em soluções de alto custo.

A demonstração prática realizada em ambiente controlado reforçou esse cenário ao evidenciar como uma vulnerabilidade conhecida e amplamente documentada pode ser identificada e explorada utilizando ferramentas gratuitas e amplamente disponíveis na comunidade de segurança ofensiva. Em poucos minutos foi possível identificar serviços vulneráveis, confirmar a existência de uma falha conhecida e obter acesso privilegiado ao sistema-alvo. Esse resultado demonstra que a exploração de vulnerabilidades nem sempre exige recursos avançados por parte dos atacantes, especialmente quando não existem processos adequados de atualização e monitoramento.

Outro aspecto observado durante o desenvolvimento deste trabalho foi a viabilidade da utilização de ferramentas gratuitas como Nmap, OpenVAS, Wireshark, OWASP ZAP e Metasploit Framework. Embora algumas dessas ferramentas exijam conhecimento técnico para interpretação dos resultados, elas oferecem recursos suficientes para apoiar atividades de reconhecimento, análise de vulnerabilidades e validação de riscos sem a necessidade de investimentos elevados em licenciamento de software.

Os resultados observados corroboram a hipótese de que práticas de segurança ofensiva podem ser adaptadas à realidade das PMEs sem comprometer o rigor técnico. A utilização de ferramentas gratuitas, associada à aplicação de metodologias reconhecidas pelo mercado, demonstrou que a identificação e validação de vulnerabilidades não dependem exclusivamente de soluções comerciais de alto custo. Dessa forma, o modelo proposto apresenta potencial para ampliar o acesso de pequenas e médias empresas a processos estruturados de avaliação de segurança.

6.1 BENEFÍCIOS DA PROPOSTA

Entre os principais benefícios identificados, destaca-se a possibilidade de implementar práticas de segurança ofensiva de forma gradual e compatível com a realidade financeira das PMEs. O modelo proposto não depende exclusivamente da contratação de especialistas altamente qualificados, permitindo que profissionais em início de carreira, como estagiários ou analistas juniores, participem das atividades de menor complexidade enquanto empresas especializadas executam avaliações mais avançadas.

Outro benefício relevante é a utilização de ferramentas de baixo custo ou gratuitas, reduzindo significativamente as barreiras de entrada para a adoção de processos de segurança. Além disso, o modelo contribui para aumentar a conscientização organizacional sobre riscos reais, transformando vulnerabilidades abstratas em evidências concretas que podem orientar decisões de investimento e melhoria da infraestrutura.

Adicionalmente, destaca-se a possibilidade de adoção gradual de controles defensivos compatíveis com a realidade das PMEs. Soluções de mercado voltadas para pequenas empresas, como serviços gerenciados de segurança e plataformas de proteção de endpoints baseadas em assinatura, permitem complementar as atividades de Pentest sem exigir grandes investimentos iniciais em infraestrutura ou equipes especializadas. Isso favorece a construção progressiva da maturidade em segurança da informação, reduzindo barreiras de entrada para organizações com recursos limitados.

6.2 LIMITAÇÕES DA PROPOSTA

Apesar dos resultados positivos, algumas limitações devem ser consideradas. A principal delas é que a validação do modelo foi realizada em ambiente controlado de laboratório, utilizando uma máquina propositalmente vulnerável. Dessa forma, os resultados obtidos não representam integralmente a complexidade encontrada em ambientes corporativos reais.

Outra limitação está relacionada à dependência do comprometimento da organização com a implementação das correções recomendadas. A simples identificação das vulnerabilidades não garante a melhoria da segurança caso não

existam recursos, planejamento ou interesse por parte da empresa para corrigir os problemas encontrados.

Além disso, embora a utilização de profissionais em início de carreira contribua para a redução de custos, a efetividade dessa abordagem depende da capacitação contínua desses colaboradores e da existência de processos bem definidos. A falta de treinamento adequado pode comprometer a qualidade das atividades executadas e limitar os benefícios esperados pelo modelo.

Também deve ser considerada a limitação sobre o escopo do modelo proposto. A abordagem concentra-se principalmente na identificação, validação e mitigação de vulnerabilidades técnicas por meio de atividades de Pentest. Dessa forma, não contempla integralmente práticas mais avançadas de segurança ofensiva, como exercícios de Red Team, simulações completas de ameaças persistentes avançadas (APT), testes extensivos de engenharia social ou avaliações aprofundadas da capacidade de detecção e resposta da organização. Embora essas atividades possam proporcionar uma visão mais abrangente da postura de segurança, sua implementação geralmente demanda recursos financeiros, tempo e especialização incompatíveis com a realidade da maioria das PMEs.

Apesar dessas limitações, elas não comprometem o objetivo principal da pesquisa, que consiste na proposição e demonstração de um modelo conceitual adaptado à realidade das PMEs. A validação em ambiente controlado permitiu demonstrar, de forma segura e reproduzível, a aplicação das etapas propostas. Entretanto, reconhece-se que a ausência de aplicação prática em uma PME real constitui a principal limitação metodológica do estudo e representa uma oportunidade para pesquisas futuras voltadas à validação empírica do modelo em ambientes organizacionais reais.

6.3 CONSIDERAÇÕES SOBRE OS RESULTADOS

De forma geral, os resultados obtidos indicam que a adoção de práticas de Pentest em PMEs é tecnicamente viável e pode ser implementada de maneira gradual utilizando recursos acessíveis. A combinação entre profissionais internos, ferramentas gratuitas e serviços especializados terceirizados mostrou-se uma alternativa compatível com as limitações normalmente encontradas nesse tipo de organização. Embora existam desafios relacionados à capacitação, aos custos e à necessidade de

validação em ambientes reais, o modelo proposto apresenta potencial para contribuir com a melhoria da postura de segurança das PMEs brasileiras, oferecendo uma abordagem estruturada e financeiramente mais acessível para a identificação e mitigação de vulnerabilidades.

6.4 COMPARAÇÃO DE MODELOS

A realização de Pentests em organizações de grande porte normalmente envolve equipes especializadas, ferramentas comerciais e processos formais de segurança já estabelecidos. Embora essa abordagem proporcione elevado nível de profundidade técnica, sua adoção pode ser limitada em pequenas e médias empresas devido aos custos envolvidos e à escassez de profissionais especializados.

O modelo proposto nesta pesquisa busca reduzir essas barreiras ao combinar ferramentas gratuitas, capacitação gradual de profissionais internos e contratação pontual de serviços especializados. Em vez de depender exclusivamente de uma equipe dedicada de segurança ofensiva, a proposta distribui responsabilidades entre diferentes atores, permitindo que as atividades de identificação, validação e mitigação de vulnerabilidades sejam realizadas de forma compatível com a realidade operacional das PMEs.

Diante disso, os resultados obtidos ao longo desta pesquisa indicam que o modelo proposto não pretende substituir abordagens tradicionais utilizadas por organizações com maior maturidade em segurança da informação. Em vez disso, busca oferecer uma alternativa viável para PMEs que, em muitos casos, não possuem condições financeiras ou estruturais para adotar processos completos de segurança ofensiva. Dessa forma, a proposta amplia o acesso a práticas de Pentest sem comprometer os princípios metodológicos fundamentais da atividade.

Além disso, a integração entre Pentest, correção das vulnerabilidades e monitoramento contínuo representa um diferencial em relação a abordagens focadas exclusivamente na identificação de falhas. Ao incorporar mecanismos de acompanhamento e mitigação ao longo do tempo, o modelo favorece a evolução gradual da maturidade de segurança das PMEs, contribuindo para a redução contínua de riscos e para o fortalecimento da resiliência organizacional.

7 CONSIDERAÇÕES FINAIS

Esta pesquisa investigou como metodologias de Pentest podem ser adaptadas à realidade das pequenas e médias empresas brasileiras como estratégia de fortalecimento da segurança da informação. O percurso desenvolvido, desde a fundamentação teórica até a demonstração prática em laboratório virtual controlado, permitiu responder satisfatoriamente à questão de pesquisa estabelecida. Os resultados obtidos indicam que práticas de segurança ofensiva podem ser adaptadas ao contexto das PMEs de forma metodologicamente estruturada, tecnicamente consistente e financeiramente viável.

Os objetivos específicos definidos para o trabalho foram alcançados. Inicialmente, foram apresentados os fundamentos teóricos da segurança ofensiva e do Pentest com base em referências acadêmicas e normativas reconhecidas. Em seguida, discutiram-se os principais desafios enfrentados pelas PMEs na adoção dessas práticas. A partir dessa análise, foi desenvolvida uma estrutura conceitual composta por cinco fases, fundamentada nos frameworks PTES, MITRE ATT&CK e Cyber Kill Chain. Complementarmente, foi proposto um arranjo operacional dividido em três camadas, distribuindo responsabilidades entre recursos internos e serviços especializados com o objetivo de compatibilizar a aplicação do modelo às limitações financeiras e estruturais frequentemente presentes nesse segmento. Por fim, a demonstração prática realizada em laboratório virtual permitiu ilustrar a aplicação das etapas de reconhecimento, análise de vulnerabilidades e exploração controlada por meio de ferramentas gratuitas amplamente disponíveis.

Os resultados obtidos reforçam a premissa de que a identificação e validação de vulnerabilidades não dependem exclusivamente de soluções comerciais ou de equipes altamente especializadas. A combinação entre metodologias reconhecidas, ferramentas acessíveis e processos estruturados demonstrou potencial para ampliar a adoção de práticas de avaliação de segurança por PMEs, aproximando organizações de pequeno porte de mecanismos tradicionalmente mais presentes em empresas de maior maturidade tecnológica.

Entretanto, o Pentest não deve ser compreendido como solução suficiente para todos os desafios relacionados à segurança da informação. Sua principal contribuição está na identificação de vulnerabilidades, validação de riscos e geração de informações capazes de subsidiar processos de tomada de decisão. Aspectos

relacionados à cultura organizacional de segurança, conscientização de usuários, monitoramento contínuo, resposta a incidentes e proteção contra ameaças avançadas exigem abordagens complementares. Nesse sentido, o Pentest deve ser entendido como parte integrante de uma estratégia mais ampla de gestão da segurança da informação.

Algumas limitações também devem ser consideradas. A principal delas refere-se à validação da proposta em laboratório virtual controlado, utilizando uma máquina intencionalmente vulnerável. Embora essa abordagem tenha permitido ilustrar a aplicação prática das etapas definidas de forma segura e reproduzível, ela não representa integralmente a complexidade encontrada em ambientes corporativos reais. Além disso, o modelo concentra-se predominantemente na identificação e validação de vulnerabilidades técnicas, não contemplando de forma abrangente atividades mais avançadas, como exercícios de Red Team, testes extensivos de engenharia social ou avaliações aprofundadas da capacidade de detecção e resposta das organizações.

Como continuidade desta pesquisa, a aplicação prática do modelo proposto em PMEs reais constitui a etapa mais imediata e relevante, permitindo avaliar sua viabilidade operacional em diferentes contextos organizacionais e comparar os resultados obtidos em laboratório com cenários corporativos reais. Além dessa validação empírica, pesquisas futuras poderão explorar diferentes direções, incluindo a adoção de exercícios de Purple Team em PMEs, nos quais equipes ofensivas e defensivas atuam de forma colaborativa; a implementação de práticas de Continuous Pentesting para monitoramento periódico de novas vulnerabilidades; a integração de técnicas de Inteligência Artificial aos processos de Pentest, especialmente na correlação de vulnerabilidades e priorização de riscos; a adoção progressiva de arquiteturas Zero Trust em ambientes de pequeno porte; e o desenvolvimento de plataformas acessíveis de automação da gestão de vulnerabilidades baseadas em ferramentas de código aberto. Essas possibilidades configuram uma agenda de pesquisa relevante e alinhada às tendências contemporâneas da segurança ofensiva aplicada ao contexto organizacional brasileiro.

A contribuição central deste trabalho para a área de Segurança da Informação consiste na proposição de um modelo conceitual adaptado à realidade das PMEs brasileiras, tornando práticas de Pentest mais acessíveis a organizações que frequentemente enfrentam limitações financeiras e técnicas. Em um cenário marcado

pelo crescimento contínuo das ameaças cibernéticas e pela elevada exposição das pequenas e médias empresas a riscos digitais, a disponibilização de processos estruturados, acessíveis e compatíveis com suas necessidades representa não apenas uma contribuição acadêmica, mas também uma iniciativa com potencial impacto econômico e social.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2022:** tecnologia da informação – segurança da informação, segurança cibernética e proteção à privacidade – sistemas de gestão da segurança da informação – requisitos. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2022:** tecnologia da informação – segurança da informação, segurança cibernética e proteção à privacidade – controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27032:2023:** cibersegurança – diretrizes para segurança da internet. Rio de Janeiro: ABNT, 2023.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos. Brasília, DF: Presidência da República, 2012. Disponível em: <www.planalto.gov.br>. Acesso em: 18 abr. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: <www.planalto.gov.br>. Acesso em: 26 abr. 2026.

BRYNIELSSON, J. et al. Cyber situational awareness in the military domain. In: IEEE MILITARY COMMUNICATIONS CONFERENCE – MILCOM, 2014, Washington. **Proceedings [...].** Washington: IEEE, 2014.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Estatísticas dos incidentes reportados ao CERT.br – 2023.** São Paulo: NIC.br, 2024. Disponível em: <www.cert.br/stats>. Acesso em: 14 mar. 2026.

ENISA – EUROPEAN UNION AGENCY FOR CYBERSECURITY. **ENISA Threat Landscape 2023.** Athens: ENISA, 2023. Disponível em: <www.enisa.europa.eu>. Acesso em: 21 mar. 2026.

GIL, A. C. **Como elaborar projetos de pesquisa.** 4. ed. São Paulo: Atlas, 2002.
HERZOG, P. **OSSTMM: Open-Source Security Testing Methodology Manual.** Version 3. Barcelona: ISECOM, 2010. Disponível em: <www.isecom.org>. Acesso em: 11 fev. 2026.

HUTCHINS, E. M.; CLOPPERT, M. J.; AMIN, R. M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In: INTERNATIONAL CONFERENCE ON INFORMATION WARFARE AND SECURITY, 6., 2011, Reading. **Proceedings [...].** Reading: Academic Publishing, 2011.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **Estatísticas do Cadastro Central de Empresas – CEMPRE 2022.** Rio de Janeiro: IBGE, 2022. Disponível em: <www.ibge.gov.br>. Acesso em: 27 mar. 2026.

KASPERSKY. **PMEs recebem 365 tentativas de ataque por minuto no Brasil: veja como se proteger.** 2024. Disponível em: <www.kaspersky.com.br/about/press-releases/kaspersky-pmes-recebem-365-tentativas-de-ataque-por-minuto-no-brasil-veja-como-se-proteger>. Acesso em: 24 mar. 2026.

KENNEDY, D. et al. **Metasploit: the penetration tester's guide.** San Francisco: No Starch Press, 2011.

MINAYO, M. C. S. **O desafio do conhecimento: pesquisa qualitativa em saúde.** 14. ed. São Paulo: Hucitec, 2014.
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Special Publication 800-115: technical guide to information security testing and assessment.** Gaithersburg: NIST, 2008.

NOGUEIRA, M. **O impacto da cibersegurança nas pequenas e médias empresas brasileiras**. SBC Horizontes, [S. l.], 4 mar. 2025. Disponível em: https://horizontes.sbc.org.br/index.php/2025/03/o-impacto-da-ciberseguranca-nas-pequenas-e-medias-empresas-brasileiras/. Acesso em: 9 abr. 2026.

PENETRATION TESTING EXECUTION STANDARD. **PTES Technical Guidelines.** 2012. Disponível em: <www.pentest-standard.org>. Acesso em: 29 jan. 2026.
STALLINGS, W. **Cryptography and network security: principles and practice.** 7. ed. Hoboken: Pearson, 2017.

STROM, B. E. et al. **MITRE ATT&CK: design and philosophy.** McLean: MITRE Corporation, 2020. Disponível em: <attack.mitre.org>. Acesso em: 16 fev. 2026.

VERIZON. **2023 Data Breach Investigations Report (DBIR).** New York: Verizon Business, 2023. Disponível em: <www.verizon.com/business/resources/reports/dbir>. Acesso em: 05 abr. 2026.

WHITMAN, M. E.; MATTORD, H. J. **Principles of information security.** 7. ed. Mason: Cengage Learning, 2022.

ZENKO, M. **Red team: how to succeed by thinking like the enemy.** New York: Basic Books, 2015.