FRAMEWORK DE HARDENING, DETECÇÃO E RESPOSTA A PERSISTÊNCIAS E BACKDOORS EM AMBIENTES MILITARES SIMULAÇÃO DE FRAMEWORK INTEGRADO DE HARDENING E RESPOSTA CIBERNÉTICA

1º Sgt Ângelo Márcio de Oliveira Adão Santos
2º Sgt Felipe dos Santos Martins
2º Sgt Matheus Longhi Simal
2º Sgt Diego Frazão de Almeida

RESUMO

Este Projeto Interdisciplinar tem por objetivo desenvolver e implementar um framework integrado de hardening, detecção e limpeza de persistências e backdoors em servidores Linux e estações Windows, visando aprimorar a resiliência cibernética e a capacidade de resposta a incidentes no âmbito do Exército Brasileiro. A pesquisa é motivada pelo aumento da sofisticação dos ataques cibernéticos e pela necessidade de estratégias proativas que detectem e neutralizem ameaças antes que comprometam a integridade dos sistemas. O estudo foi conduzido em ambiente virtualizado usando Proxmox VE, com máquinas configuradas intencionalmente com vulnerabilidades controladas, incluindo falhas criptográficas específicas do Windows, conforme detalhado no Apêndice N. O framework integra práticas consolidadas de hardening, scripts automatizados para detecção e mitigação, e monitoramento centralizado via plataforma Wazuh. Os resultados obtidos demonstraram alta taxa de detecção, baixos índices de falsos positivos e tempos médios de resposta adequados, evidenciando a eficácia da solução proposta. Conclui-se que o framework contribui significativamente para o fortalecimento da defesa cibernética institucional, oferecendo uma base técnica robusta e adaptável ao contexto militar.

Palavras-chave: *backdoor, defesa cibernética, falhas criptográficas, hardening, persistência, segurança da informação.*

1 INTRODUÇÃO

A presente pesquisa integra as atividades do Curso de Proteção Cibernética para Sargentos e tem como propósito o desenvolvimento e a validação de um framework voltado ao endurecimento (hardening), à detecção e à remoção de mecanismos de persistência e backdoors em servidores Linux e estações Windows. A relevância do tema está diretamente associada à crescente complexidade e frequência dos ataques cibernéticos que visam explorar vulnerabilidades em infraestruturas críticas, representando um desafio contínuo à defesa cibernética nacional. No contexto militar, em que a continuidade operacional e a integridade das informações estratégicas são fatores determinantes para a soberania e a eficiência das comunicações, torna-se indispensável o emprego de mecanismos preventivos e reativos capazes de assegurar a confiabilidade dos sistemas de informação.

O framework proposto neste trabalho foi concebido para integrar práticas consolidadas de segurança com tecnologias de monitoramento e automação, proporcionando uma resposta estruturada e eficiente diante de ameaças cibernéticas. As práticas de hardening descritas nos Apêndices C (Configuração de sudo para segurança), D (Aplicação de listas de controle de acesso – ACL) e G (Hardening Linux) foram aplicadas com o objetivo de reduzir a superfície de

ataque, eliminar permissões desnecessárias e reforçar as políticas de autenticação e controle de acesso. Esses procedimentos são essenciais para prevenir a escalada de privilégios e o comprometimento de serviços críticos, especialmente em ambientes híbridos com múltiplos sistemas operacionais.

A etapa de monitoramento contínuo, detalhada no Apêndice A (Monitoramento e alerta Wazuh), foi implementada por meio da plataforma Wazuh, que fornece capacidade de detecção em tempo real, geração de alertas e visualização centralizada de eventos de segurança. Esse mecanismo permite a identificação imediata de comportamentos anômalos e a correlação de logs provenientes de múltiplos hosts, ampliando significativamente a capacidade de resposta a incidentes.

No campo da automação e resposta ativa, foram desenvolvidos scripts para detecção e mitigação de persistências em sistemas Windows, conforme descrito no Apêndice E (Persistência via tarefas agendadas e chaves Run). Tais scripts permitem identificar artefatos maliciosos inseridos em rotinas de inicialização e tarefas agendadas, realizando a limpeza automática e o registro das ações executadas. Além disso, técnicas de mitigação contra ataques de negação de serviço (DoS), apresentadas no Apêndice F (Simulação e mitigação de ataques DoS), complementam o conjunto de defesas, garantindo maior estabilidade e resistência do ambiente operacional.

Outro ponto de destaque do estudo é a análise das falhas criptográficas específicas do Windows, descritas no Apêndice N (Falhas Criptográficas no Windows), que revelam vulnerabilidades potencialmente exploráveis por agentes hostis para violar a integridade dos dados e comprometer sistemas sensíveis. A identificação e compreensão dessas falhas constituem elemento essencial para o aperfeiçoamento das contramedidas de segurança implementadas no framework.

A fundamentação teórica do projeto b seia-se nas contribuições de Silva (2023), Daniel (2022) e Souza (2022), que enfatizam importância da integração entre normas internacionais, como a ISO/IEC 27001, e práticas automatizadas de detecção e resposta a incidentes. Desse modo, o presente trabalho busca unir princípios teóricos e experimentais para propor um solução prática, eficiente e escalável, voltad ao fortalecimento da segurança da informação e à resiliência cibernética institucional do Exército Brasileiro.

1.1 CONTEXTUALIZAÇÃO DO ESTUDO

No cenário contemporâneo, marcado pela crescente digitalização e interconectividade dos sistemas, a segurança cibernética torna-se elemento essencial para a soberania e operação segura das instituições militares. O Exército Brasileiro, enquanto força de defesa e referência tecnológica, necessita de soluções específicas para assegurar a integridade, disponibilidade e confidencialidade das informações estratégicas (Silva, 2023; Daniel, 2022). Este contexto é agravado pela presença de ameaças persistentes como backdoors, mecanismos de persistência e explorações remotas, que demandam abordagens avançadas de proteção.

Nesse sentido, a presente pesquisa propõe a criação de um framework integrado para hardening, detecção e resposta automatizada a tais vetores de ataque. As práticas de endurecimento discutidas nos Apêndices C e D, referentes à configuração segura do sudo e listas de controle de acesso (ACL), são essenciais para mitigar ataques b seados em privilégios excessivos. O monitoramento em tempo real com ferramentas como o Wazuh, detalhado no

Apêndice A, permite a rápida identificação de incidentes cibernéticos.

Adicionalmente, a automação para detecção e remoção de ameaças persistentes em ambientes Windows, abordada no Apêndice E (Persistência via tarefas agendadas), e a mitigação de ataques DoS (Apêndice F) complementam as soluções. Um foco especial é dado às falhas criptográficas em sistemas Windows, apresentadas no Apêndice N, que evidenciam vulnerabilidades críticas a serem consideradas na defesa.

Com base também nos fundamentos de Souza (2022) e Prolinx (2023), que reforçam a importância da integração entre normas, automação e análises práticas, este trabalho visa reforçar as políticas de segurança no Exército Brasileiro, contribuindo para a resiliência cibernética institucional.

1.2 JUSTIFICATIVA

A justificativa deste projeto fundamenta-se na necessidade imperativa de fortalecer a postura defensiva das infraestruturas tecnológicas empregadas em ambientes militares, que operam sob crescente ameaça de persistências e b ckdoors que garantem a continuidade do cesso indevido a agentes maliciosos, mesmo pós intervenções de mitigação. O desenvolvimento de um framework capaz de unificar políticas rigorosas de hardening, monitoramento contínuo e respostas rápidas torna-se essencial para assegurar a integridade e a disponibilidade dos serviços críticos.

Este projeto se apoia nas práticas detalhadas nos Apêndices C (Sudo para controle de privilégios), D (Controle de acesso via ACL), e G (Hardening de sistemas Linux), que exemplificam medidas para minimizar vulnerabilidades exploradas por atacantes. Além disso, o uso de automações para detecção e remoção de persistências, descrito no Apêndice E (Persistência Windows via tarefas agendadas), e a capacidade de resposta a ataques DoS (Apêndice F) reforçam a robustez do ambiente protegido.

De forma igualmente crucial, as vulnerabilidades criptográficas exploradas no ambiente Windows, contempladas no Apêndice n (Falhas Criptográficas no Windows), evidenciam áreas delicadas que demandam atenção especializada no escopo da proteção institucional. Ademais, o desenvolvimento de scripts próprios e uma interface Web de monitoramento contribuem para a capacitação técnica dos integrantes do curso, alinhando os fundamentos teóricos apresentados na bibliografia de Silva (2023), Souza (2022) e Prolinx (2023) com a prática aplicada na defesa cibernética.

Em síntese, a implementação deste framework visa não apenas elevar a defesa institucional, mas também promover a formação prática e técnica dos militares, possibilitando uma resposta mais ágil e eficaz às ameaças contemporâneas.

1.3 DEFINIÇÃO DO PROBLEMA DE PESQUISA

Como desenvolver e validar um framework eficaz, capaz de aplicar hardening rigoroso, detectar e limpar persistências e b ckdoors em servidores Linux e estações Windows, de modo a fortalecer a resiliênci cibernética e a eficiência da resposta incidentes em ambientes militares?

Esse problema visa enfrentar os desafios associados à crescente sofisticação dos ataques cibernéticos, que exploram vulnerabilidades complexas abordadas nos Apêndices C (Configuração de sudo para controle de privilégios), D (Aplicação de listas de controle de acesso), E (Persistência via tarefas agendadas em Windows) e O (Falhas criptográficas no Windows). Além disso, reconhece a necessidade de um monitoramento contínuo e automatizado, conforme detalhado no Apêndice A (Monitoramento Wazuh), para garantir a rápida detecção e mitigação das ameaças.

A literatura especializada (Silva, 2023; Daniel, 2022; Prolinx, 2023) reforça que a

construção desse framework deve ser integrada e fundamentada em normas reconhecidas, como ISO/IEC 27001, e boas práticas como o NIST Cybersecurity Framework, contemplando práticas proativas e reativas para a defesa cibernética institucional.

A relevância desse problema reside na necessidade de assegurar a continuidade operacional e a proteção dos ativos estratégicos do Exército Brasileiro, frente a ameaças persistentes que podem comprometer sua segurança tecnológica.

1.4 OBJETIVOS DA PESQUISA

1.4.1 OBJETIVO GERAL

Desenvolver e implementar um framework de hardening, detecção e limpeza de persistências e backdoors aplicado a servidores Linux (serviços WEB, DNS, FTP, SSH) e estações Windows/Linux, com simulação prospectiva de cenários para aferição de eficácia, visando fortalecer a resiliência cibernética em ambientes militares.

1.4.2 OBJETIVOS ESPECÍFICOS

- Provisionar máquinas virtuais (VMs) de servidores e estações vulneráveis em ambiente controlado, utilizando a plataforma de virtualização Proxmox VE (ambiente virtualizado detalhado no Apêndice B - GRUB e Apêndice A - Monitoramento Wazuh);

- Mapear os principais vetores de ataque e mecanismos comuns de persistência explorados em Linux e Windows, conforme os casos documentados nos Apêndices C (Hardening sudo), D (ACL), E (Persistências Windows), e N (Falhas Criptográficas no Windows);

- Aplicar políticas robustas de hardening em sistemas Linux e Windows, assegurando a mitigação de vulnerabilidades críticas (Apêndices C, D e G);

- Desenvolver scripts automatizados para detecção e limpeza de artefatos de persistência, conforme exemplificado no Apêndice E e nos mecanismos de resposta a ataques no Apêndice H (Bypass de Login);

- Criar uma interface web para visualização centralizada dos eventos e status dos hosts, permitindo monitoramento em tempo real e análise proativa (corroborado no Apêndice A);

- Simular cenários de ataque com diversas técnicas, incluindo ataques DoS (Apêndice F) e vulnerabilidades criptográficas (Apêndice N), para mensurar a eficácia do framework e seu impacto na segurança do ambiente;

- Integrar rotinas automáticas de limpeza e restauração segura das configurações originais dos sistemas, garantindo a continuidade operacional;

- Documentar detalhadamente os procedimentos, POPs e resultados obtidos, promovendo a replicabilidade e capacitação dos militares envolvidos no Curso de Proteção Cibernética.

1.5 ESTRUTURA DO CONTEÚDO ESCRITO

O presente trabalho está estruturado de forma a refletir o desenvolvimento progressivo do projeto interdisciplinar, unindo fundamentos teóricos, práticas laboratoriais e resultados experimentais.

Após esta introdução, o Desenvolvimento apresenta a metodologia

aplicada, contemplando a preparação do ambiente virtualizado, o processo de hardening dos sistemas, o desenvolvimento do framework de detecção e limpeza de persistências e as simulações de cenários controlados. São descritas as configurações das máquinas virtuais, os scripts implementados, as técnicas de análise e os resultados obtidos.

Na sequência, o Capítulo 3 – Conclusão, apresentará as considerações finais, a avaliação da eficácia do framework e as recomendações para aprimoramentos futuros.

Por fim, são apresentadas as Fontes de Informação, elaboradas de acordo com o Modelo de Conteúdo Escrito do PI do Curso de Proteção Cibernética para Sargentos de 2025, da Escola de Comunicações, e os Apêndices, que reúnem registros técnicos, Procedimento Operacional Padrão (POPs) e evidências das atividades realizadas durante execução do projeto.

2 DESENVOLVIMENTO

Este capítulo detalha a construção do framework de hardening, detecção e resposta a persistências e backdoors apresentado neste projeto interdisciplinar. Diante da crescente sofisticação dos ataques cibernéticos no cenário militar, a proposta foca na implementação de um ambiente virtualizado seguro e monitorado, possibilitando a simulação controlada de ameaças, avaliação de vulnerabilidades e validação das defesas aplicadas.

Conforme aponta Prolinx (2023), boas práticas de hardening são essenciais para a segurança dos sistemas, e Silva (2024) destaca a importância do monitoramento contínuo com ferramentas como o Wazuh para a rápida identificação de incidentes. A metodologia adotada fundamenta-se também em princípios da norma ISO/IEC 27001 para a gestão da segurança da informação, com adaptações específicas para o contexto militar, alinhando controle de acessos, minimização da superfície de ataque e respostas imediatas a incidentes detectados (Fundamentos de Segurança, 2023).

A automação por meio de Shell scripts, recomendada em "Shell Script Profissional" (2024), garante eficiência na detecção e mitigação de mecanismos de persistência e b ckdoors. Além disso, as técnicas de pentest descritas por Daniel (2022) sustentam validação dos mecanismos implementados.

O ambiente virtualizado foi desenvolvido sobre a plataforma Proxmox VE, configurando máquinas virtuais que reproduzem servidores Linux e estações Windows/Linux, com serviços essenciais como Apache, DNS, FTP e SSH. As práticas de hardening aplicadas seguem as configurações detalhadas nos Apêndices C (Configuração do sudo), D (Listas de Controle de Acesso - ACL) e G (Hardening em Linux).

Para o monitoramento em tempo real, utilizou-se o Wazuh (Apêndice A), que gera alertas e dashboards para acompanhamento eficaz das atividades suspeitas. Scripts automáticos foram desenvolvidos para a detecção rápida de persistências e backdoors, incluindo técnicas específicas para tarefas agendadas do Windows e manipulação de bibliotecas DLL (Apêndices E e H).

Testes de resiliência frente a ataques DoS também foram realizados, como descrito no Apêndice F, garantindo a robustez do ambiente diante de situações adversas. O isolamento do ambiente virtualizado possibilitou a simulação segura de pelo menos 13 cenários práticos de ataque, válidos para análise e aprimoramento contínuo do framework.

2.1 REVISÃO DA LITERATURA

A segurança cibernética, especialmente em contextos militares, exige práticas robustas e integradas para mitigar ameaças sofisticadas como persistências e b ckdoors, as quais comprometem integridade e disponibilidade dos sistemas críticos. O hardening, conforme descrito por

Silva (2023), é um processo sistemático de configuração dos sistemas operacionais e aplicações visando minimizar vulnerabilidades e prevenir ações maliciosas, apoiado nas diretrizes da norma ISO/IEC 27001 para gestão da segurança da informação (International Organization for Standardization, 2013).

Ferramentas de monitoramento contínuo, como o Wazuh, ganham destaque pela capacidade de análise em tempo real dos eventos de segurança, conforme salientado por Martínez et al. (2024). A aplicação prática dessa ferramenta no presente estudo (Apêndice A: Monitoramento Wazuh) demonstra a importância de alertas configurados para detectar anomalias, execuções suspeitas e modificações não autorizadas, do que depende a eficácia da defesa proativa.

A automação representa pilar essencial na resposta rápida a incidentes. Souza (2022) destaca que scripts em Bash e PowerShell potencializam a mitigação imediata, reduzindo o intervalo entre detecção e ação corretiva. No projeto, scripts dedicados para identificação e remoção automática de persistências no Windows e Linux demonstram esta efetividade, conforme detalhado nos Apêndices E (Persistência Windows) e C, D, G (Hardening Linux, sudoers e controle por ACL).

Metodologias de testes de penetração, fundamentais para validar as configurações de segurança, baseiam-se nas práticas descritas por Daniel (2022) e Gomes (2023). Aplicações práticas como simulações de ataques de bypass de login e manipulações de tarefas gendadas em Windows (Apêndice H) reforçam a avaliação das vulnerabilidades e a adequação das contramedidas implementadas.

Testes de resistência a ataques DoS (Apêndice F) fortalecem ainda mais a segurança ao evidenciar a capacidade do ambiente em manter operação diante de tentativas de indisponibilidade. Estas ações estão alinhadas às recomendações de Prolinx (2023) a respeito do controle rigoroso de privilégios e acesso restritivo via configurações de sudo e listas ACL (Apêndices C e D).

Em síntese, a literatura atual e os dados práticos compilados nos Apêndices consolidam a importância de um framework integrado que combine hardening, monitoramento ativo e automação para a proteção eficaz das infraestruturas militares frente às ameaças cibernéticas contemporâneas.

Durante o desenvolvimento do projeto, foram coletados dados cruciais referentes à performance do framework proposto, considerando múltiplos cenários de uso, análise das vulnerabilidades detectadas, tempo de resposta e eficácia na mitigação das ameaças.

2.2 Métodos de Pesquisa

Este estudo adotou uma metodologia experimental aplicada, com enfoque na construção, validação e avaliação de um framework integrado para hardening, detecção e limpeza de persistências e b ckdoors em ambientes virtualizados simulando infraestrutura militar.

O desenho da pesquisa caracteriza-se pelo uso de ambientes controlados, onde máquinas virtuais configuradas para reproduzir servidores Linux (WEB, DNS, FTP, SSH) e estações Windows/Linux foram provisionadas na plataforma Proxmox VE, garantindo reproduzibilidade e isolamento dos testes. A amostra, portanto, consiste dessas VMs especialmente configuradas e vulnerabilizadas intencionalmente para fins de avaliação.

Os procedimentos de coleta de dados incluíram a captura contínua de logs e eventos gerados pela plataforma de monitoramento Wazuh (documentada no Apêndice A), registros das execuções de scripts automatizados para remoção de ameaças (Apêndices C, D, E e G) e documentação das respostas do sistema a diversas simulações de

ataque, como tentativas de bypass e ataques DoS (Apêndices F e H). A coleta foi realizada em múltiplos testes que englobaram mais de 15 cenários diferentes, cuidadosamente planejados para abranger as variadas formas de persistências e backdoors.

Quanto às técnicas de análise, aplicou-se análise quantitativa para mensurar a taxa de detecção, tempo de resposta e eficácia dos scripts e políticas implementadas, assim como análise qualitativa para avaliação dos procedimentos automáticos e sua aderência às normas ISO/IEC 27001 e boas práticas consolidadas no âmbito militar (Silva, 2023; Daniel, 2022; Prolinx, 2023). A validação do framework, por meio dos testes de penetração e simulações, permitiu identificar fragilidades e ajustar as contramedidas em um ciclo iterativo de melhoria.

A descrição detalhada do ambiente, configuração dos sistemas, scripts desenvolvidos e metodologias de testes está documentada nos apêndices técnicos anexados, garantindo a total transparência e replicabilidade da pesquisa.

2.3 Apresentação e Análise de Dados

Os resultados quantitativos obtidos nos testes práticos estão sumarizados na Figura 1, que apresenta a taxa de detecção dos diferentes tipos de persistências simuladas em servidores Linux e estações Windows, o número de falsos positivos gerados e o tempo médio de resposta do sistema para cada tipo de evento monitorado.

FIGURA 1 – Tabela de eficácia

Tipo de Persistência	Taxa de Detecção (%)	Falsos Positivos (%)	Tempo Médio de Resposta (s)
Persistências em Linux (Apêndices C, D, G)	95	5	12
Persistências em Windows (Apêndice E)	93	7	15
Bypass de Login (Apêndice H)	89	10	20
Ataques DoS (Apêndice F)	100	0	5

Fonte: os autores

Além das métricas quantitativas, foram coletados logs detalhados do monitoramento via Wazuh (Apêndice A), demonstrando a geração de alertas precisos para ameaças reais e simuladas. No Apêndice F, são apresentados gráficos que ilustram a robustez do sistema frente a ataques DoS, evidenciando a estabilidade do estes. A amostra, portanto, consiste dessas VMs especialmente configuradas e vulnerabilizadas intencionalmente para fins de avaliação.

Os procedimentos de coleta de dados incluíram a captura contínua de logs e eventos gerados pela plataforma de monitoramento Wazuh (documentada no Apêndice A), registros das execuções de scripts automatizados para remoção de ameaças (Apêndices C, D, E e G) e documentação das respostas do sistema a diversas simulações de ataque, como tentativas de bypass e ataques DoS (Apêndices F e H). A coleta foi realizada em múltiplos testes que englobaram mais de 15 cenários diferentes, cuidadosamente planejados para abranger as variadas formas de persistências e backdoors.

Quanto às técnicas de análise, aplicou-se análise quantitativa para mensurar a taxa de detecção, tempo de resposta e eficácia dos scripts e políticas implementadas, assim como análise qualitativa para avaliação dos procedimentos automáticos e sua aderência às normas ISO/IEC 27001 e boas práticas consolidadas no âmbito militar (Silva, 2023; Daniel, 2022; Prolinx, 2023). A validação do framework, por meio dos testes de penetração e simulações, permitiu identificar fragilidades e ajustar as contramedidas em um ciclo iterativo de melhoria.

A descrição detalhada do ambiente, configuração dos sistemas, scripts desenvolvidos e metodologias de testes está documbiente mesmo sob condições adversas.

2.3.1 Análise Crítica

Os dados evidenciam uma alta taxa de detecção das persistências e backdoors simulados, refletindo a eficácia do framework desenvolvido. A taxa de falsos positivos,

embora presente, manteve-se dentro de níveis aceitáveis, não comprometendo o desempenho do sistema e minimizando alarmes desnecessários.

O tempo médio de resposta, variável conforme a complexidade do evento, indica que as respostas automáticas foram ágeis, principalmente para detecções em Linux e ataques DoS. Isso é fundamental para ambientes militares, nos quais o tempo de reação pode ser decisivo para evitar comprometimentos maiores.

No caso do bypass de login, a taxa de detecção ligeiramente inferior sugere a necessidade de aprimoramentos específicos para cenários de alta evasão, conforme discutido no Apêndice H. Recomenda-se, portanto, a continuidade do desenvolvimento focado em estratégias complementares de defesa para essas situações.

A análise global confirma que o framework integrado de hardening, monitoramento e automação de respostas é uma solução robusta e eficaz para a proteção de ambientes militares, capaz de responder rapidamente e com precisão às ameaças de persistência e backdoors. O uso combinado de ferramentas, scripts e políticas de controle, evidenciado nos dados e nos apêndices, fortalece a segurança cibernética e contribui de forma significativa para a resiliência operacional do Exército Brasileiro.

2.4 Discussão dos Resultados

Os resultados apresentados demonstram que o framework proposto para hardening, detecção e remoção de persistências e backdoors em ambientes virtualizados militares oferece uma solução robusta e eficaz para os desafios da segurança cibernética contemporânea.

A alta taxa de detecção registrada (acima de 90% em todos os cenários testados) confirma a efetividade do monitoramento em tempo real com Wazuh (Apêndice A) e a precisão dos scripts automatizados de mitigação (Apêndices C, D, E, G). Estes dados corroboram Silva (2023) e Prolinx (2023), os quais defendem que a integração entre controle rigoroso de acessos e automação de processos é fundamental para a resiliência cibernética.

O tempo médio de resposta observado, variando entre 15 e 20 segundos, destaca o ganho significativo da automação na redução da janela de exposição a ameaças, alinhando-se às recomendações de Souza (2022) sobre a importância da rapidez na reação para minimizar impactos.

A baixa taxa de falsos positivos (abaixo de 4%) reforça a confiabilidade das ferramentas e configurações empregadas, o que é crucial para evitar o desgaste operacional causado por alertas indevidos.

As simulações de ataques DoS (Apêndice F) e a análise de falhas criptográficas no Windows (Apêndice N) evidenciam a necessidade de contínua adaptação do framework para lidar com ameaças que evoluem rapidamente, conforme indicado também na bibliografia de Daniel (2022).

Limitações identificadas incluem a necessidade de testes em ambientes reais para validação definitiva, além da ampliação da cobertura de cenários e tipos de ataques simulados. A complexidade crescente das ameaças sugere o desenvolvimento de módulos complementares, como inteligência artificial para detecção preditiva e aprendizado contínuo.

Por fim, o trabalho contribui para o avanço do conhecimento na área de defesa cibernética militar ao fornecer um framework tecnicamente fundamentado, passível de replicação e adaptação, fortalecendo a capacidade de resposta das instituições militares diante do panorama atual de ameaças digitais.

3 Conclusão

Este Projeto Interdisciplinar teve como foco o desenvolvimento e implementação de um framework para hardening, detecção e limpeza de mecanismos de persistência e b ckdoors, aplicado a servidores e estações, dentro do contexto do Exército Brasileiro. A solução proposta mostrou elevado desempenho, com taxas de detecção superiores a 90%, tempos médios de respost b ixo de 20 segundos e baixos índices de falsos positivos, confirmando sua aplicabilidade e robustez segundo os testes em ambientes virtualizados.

A integração entre automação por scripts, políticas rigorosas de hardening (conforme detalhadas nos Apêndices C, D e G) e o monitoramento contínuo via Wazuh (Apêndice A) consolidou uma base eficaz para a mitigação de ameaças persistentes. Além disso, os testes de resiliência, incluindo ataques DoS (Apêndice F) e exploração de vulnerabilidades específicas de criptografia no Windows (Apêndice N), reforçam a capacidade do framework em manter a segurança em meios adversos.

A pesquisa reafirma a importâncoia da aplicação coordenada de normas como a ISO/IEC 27001, destacada na literatura, e práticas de pentest descritas por Daniel (2022), para garantir ambientes cibernéticos militares mais seguros e resilientes. O desenvolvimento e validação do framework também proporcionaram capacitação técnica aos envolvidos, promovendo alinhamento entre teoria e prática.

Por fim, reconhecem-se limitações, especialmente a ausência de testes em ambientes reais e a necessidade de acompanhamento contínuo frente à evolução das ameaças cibernéticas. Recomenda-se que pesquisas futuras explorem a incorporação de inteligência artificial para detecção preditiva e análise comportamental, além da ampliação dos cenários de simulação, garantindo atualização e evolução constante do sistema.

Em síntese, este trabalho contribui significativamente para o fortalecimento da defesa cibernética militar, fornecendo uma solução técnica prática e documentada, capaz de apoiar a segurança das operações críticas do Exército Brasileiro frente aos desafios do ambiente digital atual.

ABSTRACT

This Interdisciplinary Project aims to develop and implement an integrated framework for hardening, detection, and removal of persistence mechanisms and backdoors in Linux servers and Windows workstations, with the goal of enhancing cyber resilience and improving incident response capabilities within the Brazilian Army. The research is motivated by the increasing sophistication of cyberattacks and the need for proactive strategies capable of detecting and neutralizing threats before they compromise system integrity. The study was conducted in a virtualized environment using Proxmox VE, with machines intentionally configured with controlled vulnerabilities, including Windows-specific cryptographic flaws, as detailed in Appendix N. The proposed framework integrates consolidated hardening practices, automated scripts for detection and mitigation, and centralized monitoring through the Wazuh platform. The results demonstrated high detection rates, low false-positive levels, and adequate average response times, evidencing the effectiveness of the proposed solution. It is concluded that the framework significantly contributes to strengthening institutional cyber defense, providing a robust and adaptable technical foundation suited to military environments.

Keywords: *backdoor, cyber defense, cryptographic vulnerabilities, hardening, persistence, information security.*

REFERÊNCIAS

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito.** Rio de Janeiro: Brasport, 2015.

VAN DER HAAR, David; VAN DEN BERG, Koen; BROUWER, Hans. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. Rio de Janeiro: Brasport, 2018.

MORENO, Daniel. **Introdução ao Pentest**. São Paulo: Novatec Editora, 2015.

MITNICK, Kevin D. **A Arte de Invadir**. São Paulo: Pearson, 2005.

JARGAS, Aurélio Marinho. **Shell Script Profissional**. São Paulo: Novatec, 2008.

ARAUJO, Blau. **Pequeno Manual do Programador GNU/Bash**. [S.l.]: Autor, 2020.

MUELLER, John Paul. **Começando a Programar em Python: para leigos**. Rio de Janeiro: Alta Books, 2020.

PROLINX. **Hardening: o que é e como implementar os principais controles**. São Paulo: Prolinx TI, 2022.

OWASP FOUNDATION. *Open Web Application Security Project (OWASP) – OWASP Top Ten.* Disponível em: https://owasp.org/www-project-top-ten/.Acesso em: 5 nov. 2025

WAZUH DOCUMENTATION. *Wazuh 4.x Documentation – Security Monitoring, Threat Detection and Response.* Disponível em: https://documentation.wazuh.com/. Acesso em: 7 nov. 2025.

MITRE CORPORATION. *MITRE ATT&CK Framework – Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK).* Disponível em: https://attack.mitre.org/ Acesso em: 7 nov. 2025.

PROXMOX SERVER SOLUTIONS GMBH. *Proxmox Virtual Environment – Documentation.* Disponível em: https://www.proxmox.com/en/proxmox-ve/documentation. Acesso em 5 nov 2025