Análise de Severidade e Explorabilidade de Vulnerabilidades de Segurança no Setor Público

João C. C. Lima[1], Lyedson S. Rodrigues[2], Ramon S. Araújo[2], Davi C. Pinheiro[1], Rafael L. Gomes[2], Emanuel B. Rodrigues[1], Rossana M. C. Andrade[1], Clenival L. Silva[3], Daniel C. Bentes[3], Alexandre S. Cialdini[3]

[1] Universidade Federal do Ceará (UFC), Fortaleza, Ceará, Brasil.

{jcarloslima,davichavespinheiro}@alu.ufc.br,{emanuel,rossana}@dc.ufc.br

[2]Universidade Estadual do Ceará (UECE), Fortaleza, Ceará, Brasil.

{ramon.araujo,lyedson.silva}@aluno.uece.br,rafa.lopes@uece.br

[3]Secretaria do Planejamento e Gestão do Ceará (SEPLAG), Fortaleza, Ceará, Brasil.

{clenival.lopes,daniel.bentes,alexandre.cialdini}@seplag.ce.gov.br

Abstract. *The increasing sophistication of cyber threats poses challenges to the protection of public services and infrastructure, especially in heterogeneous environments. Simply detecting vulnerabilities is not enough: it is necessary to understand them in the context of the organization and prioritize remediation intelligently. This paper presents a systematic approach to vulnerability analysis based on vulnerability severity and exploitability. The methodology includes asset mapping, vulnerability scanning, CVSS and EPSS classification, and analysis between technical attributes and risks. The data were analyzed based on variables such as service ports, operating systems, severity of failures, and probability of exploitation, allowing the identification of exposure patterns and the definition of priorities. The results show that the integration of metrics and context significantly improves the effectiveness of vulnerability management in public institutions.*

Resumo. *A crescente sofisticação das ameaças cibernéticas impõe desafios à proteção de serviços e infraestruturas públicas, especialmente em ambientes heterogêneos. A simples detecção de vulnerabilidades não basta: é necessário compreendê-las no contexto da organização e priorizar a correção com inteligência. Este artigo apresenta uma abordagem sistemática de análise de vulnerabilidades baseada na severidade e explorabilidade das mesmas. A metodologia inclui mapeamento de ativos, varredura de vulnerabilidades, classificação por CVSS e EPSS, e análise entre atributos técnicos e riscos. Os dados foram analisados com base em variáveis como portas de serviço, sistemas operacionais, severidade das falhas e probabilidade de exploração, permitindo identificar padrões de exposição e definir prioridades. Os resultados mostram que a integração de métricas e contexto melhora significativamente a eficácia da gestão de vulnerabilidades em instituições públicas.*

1. Introdução

A gestão de vulnerabilidades desempenha um papel estratégico fundamental na segurança da informação em órgãos públicos, especialmente diante da crescente complexidade e heterogeneidade dos seus ambientes computacionais [Safitra et al. 2023]. Diferentemente de ambientes homogêneos e controlados, as instituições públicas costumam operar com um ecossistema diversificado de sistemas legados, aplicações modernas, equipamentos de diferentes gerações e perfis variados de usuários, desde técnicos especializados até servidores com pouca familiaridade com práticas de cibersegurança [Pimenta et al. 2024]. Especialmente no grupo de gastos de pessoal do setor público, todas as medidas de conformidade no uso da tecnologia da informação são importantes, pois trata-se de um ativo que responde por quase metade da receita corrente líquida dos estados brasileiros.

A partir deste cenário, o processo de gestão de vulnerabilidades permite identificar falhas técnicas e lacunas de configuração que poderiam ser exploradas por agentes maliciosos, colocando em risco a confidencialidade de dados sensíveis, a integridade de sistemas críticos e a continuidade dos serviços públicos [Ficco et al. 2024]. Além disso, a heterogeneidade do ambiente exige que a análise de vulnerabilidades seja realizada com uma abordagem sistemática e adaptável, capaz de contemplar diferentes sistemas operacionais, aplicações web, protocolos de rede e configurações de segurança [Silva et al. 2023]. A correlação entre métricas como o *Common Vulnerability Scoring System* (CVSS) [FIRST 2019], o *Exploit Prediction Scoring System* (EPSS) [FIRST 2022], bem como outros dados de inteligência de ameaças cibernéticas e informações contextuais do ambiente computacional, é fundamental para transformar a análise de segurança cibernética em uma atividade priorizada e eficiente [Cruz et al. 2023, Thomas et al. 2025]. Em vez de tratar vulnerabilidades de forma isolada, a correlação de diferentes variáveis de segurança permite integrar diferentes dimensões do risco e responder de maneira mais estratégica [Liu et al. 2024].

Essa prática é especialmente relevante em infraestruturas públicas complexas e dinâmicas, onde a resiliência operacional depende diretamente da capacidade de identificar, proteger e responder continuamente a riscos cibernéticos. Ela está alinhada a boas práticas internacionalmente reconhecidas, como o Cybersecurity Framework (CSF) [National Institute of Standards and Technology (NIST) 2018], que enfatiza a avaliação contínua de riscos, proteção e resposta, e os Center for Internet Security Critical Security Controls (CIS Controls) [Center for Internet Security 2023], que fornecem um conjunto priorizado de medidas defensivas contra vetores de ataque comuns.

Diante deste contexto, este artigo apresenta uma abordagem para gestão de vulnerabilidades e identificação de ativos críticos da Secretaria do Planejamento e Gestão do Ceará (SEPLAG)[1]. Considera-se ativos todos os serviços e sistemas em operação dentro da infraestrutura do órgão. A proposta vai além da simples listagem de vulnerabilidades, buscando estabelecer relações entre variáveis técnicas (tais como sistema operacional, portas de serviço e severidade das falhas) e o grau de exposição dos ativos. A abordagem permite identificar padrões de ocorrência que evidenciam fragilidades estruturais, como a presença recorrente de falhas críticas em determinados perfis de ativos. Isso se mostra especialmente relevante em instituições do setor público, onde coexistem sistemas lega-

[1] `https://www.seplag.ce.gov.br`

dos e plataformas modernas, muitas vezes sem inventário completo ou padronização de configurações.

A metodologia empregada favorece a construção de um modelo de priorização dinâmico, no qual ativos com maior densidade de vulnerabilidades, presença de *exploits* públicos e maior probabilidade de exploração (mensurada via EPSS) são destacados como críticos. Com isso, a gestão de vulnerabilidades torna-se mais eficiente e alinhada à realidade do órgão, contribuindo para decisões mais assertivas sobre ações de mitigação de ameaças, segmentação de rede e alocação de recursos de segurança cibernética.

2. Metodologia

Esta seção irá descrever a metodologia aplicada neste trabalho para a gestão de vulnerabilidades, em especial a análise de severidade e explorabilidade das mesmas.

A metodologia adotada para a gestão de vulnerabilidades seguiu princípios de melhoria contínua e priorização baseada em risco, adequando-se às restrições operacionais e ao ambiente tecnológico da instituição, sendo inspirada no *framework* de segurança cibernética do NIST [National Institute of Standards and Technology (NIST) 2018]. Esse processo estruturado foi dividido em quatro etapas principais, conforme descrito a seguir:

1. **Coleta de Informações e Mapeamento de Ativos**: Inicialmente, foi conduzido um levantamento colaborativo com a equipe técnica da instituição para identificar as faixas de rede disponíveis, os ativos mais relevantes e os períodos adequados para execução dos testes. A priorização dos *hosts* para análise considerou a viabilidade de execução diante de restrições de rede, como regras de firewall e limitações de acesso aos servidores. Além disso, *hosts* com registros PTR (*Pointer*) associados foram priorizados, por apresentarem maior probabilidade de exposição a redes externas e, portanto, representarem um risco potencialmente mais elevado. Esses critérios ajudaram a otimizar a alocação de recursos, concentrando-se em alvos com maior exposição e viabilidade de avaliação.
2. **Varredura de Vulnerabilidades**: A análise foi realizada utilizando a ferramenta de código aberto OpenVAS[2], a qual é amplamente reconhecida na comunidade de segurança para detecção de vulnerabilidades. Os testes foram executados em modo não autenticado, simulando o comportamento de um atacante externo sem credenciais válidas. Essa abordagem permitiu identificar falhas expostas diretamente na superfície de rede, respeitando as limitações operacionais e evitando impactos nos sistemas em produção. Adicionalmente, é válido ressaltar que estas ações foram realizadas fora do horário comercial, a fim de não impactar a rede de produção da instituição.
3. **Análise, Classificação e Priorização de Vulnerabilidades**: As vulnerabilidades detectadas foram classificadas com base no CVSS, atribuindo níveis de severidade (baixa, média, alta e crítica), e complementadas com a métrica EPSS, que estima a probabilidade de exploração real de cada falha. A fim de permitir uma priorização mais assertiva, também foram avaliadas a existência de *exploits* públicos e o contexto do ativo afetado (função, exposição, criticidade).

[2]`https://openvas.org`

4. **Consolidação e Monitoramento Contínuo**: Os dados gerados nas etapas anteriores foram consolidados em um documento contendo um plano de ação, permitindo à equipe técnica do órgão acompanhar a evolução das correções.

Uma das etapas mais importantes da metodologia proposta é a análise, classificação e priorização de vulnerabilidades, cujo objetivo é avaliar o grau de risco associado a cada falha identificada durante os testes de varredura. Para isso, foram utilizadas métricas consolidadas que permitem quantificar a severidade e a probabilidade de exploração das vulnerabilidades em ambientes reais.

A principal métrica adotada foi o CVSS, um sistema padronizado para mensuração da severidade de vulnerabilidades em sistemas computacionais, que atribui a cada vulnerabilidade uma pontuação de $0,1$ a $10,0$, considerando aspectos como: vetor de ataque (rede, local, físico), complexidade da exploração, privilégios necessários, impacto sobre confidencialidade, integridade e disponibilidade, entre outros. Com base nessa pontuação, as severidades das vulnerabilidades foram categorizadas da seguinte forma: Baixa ($0,1$ a $3,9$); Média ($4,0$ a $6,9$); e Alta ($7,0$ a $10,0$). Essa classificação foi automaticamente atribuída pelo OpenVAS, com base no banco de dados de vulnerabilidades conhecidas *Common Vulnerabilities and Exposures* (CVE)[3].

Complementarmente ao CVSS, a métrica EPSS estima a probabilidade de exploração de uma vulnerabilidade em ambientes reais. Essa métrica é expressa como uma pontuação entre 0 e 1, indicando a chance de que uma vulnerabilidade seja explorada por agentes maliciosos nos 30 dias seguintes à sua divulgação. O uso do EPSS permitiu diferenciar vulnerabilidades com mesma severidade CVSS, mas com níveis distintos de ameaça iminente, ajudando a direcionar ações mais urgentes. Além disso, a existência de um *exploit* (software, bloco de dados ou script de exploração) publicamente disponível em repositórios como Exploit-DB [Offensive Security 2025] ou Metasploit [Rapid7 2025] foi considerada um fator de risco adicional, pois aumenta significativamente a probabilidade de que a vulnerabilidade seja explorada por atacantes com baixo nível de sofisticação.

Por fim, é válido ressaltar que, embora o presente trabalho tenha como foco o setor público dentro de uma instituição governamental, os processos e métodos discutidos são igualmente aplicáveis a ambientes do setor privado, onde as exigências de segurança e as práticas de desenvolvimento muitas vezes refletem aquelas encontradas em organizações públicas.

3. Resultados e Discussão

Os resultados do estudo de caso apresentados nesta seção representam uma prova de conceito conduzida na SEPLAG com o objetivo de obter resultados iniciais que sirvam como base para a validação das abordagens e técnicas utilizadas. Essa etapa preliminar visa garantir a eficácia do processo antes de sua aplicação completa no ambiente real analisado, assegurando maior precisão e confiabilidade nos resultados futuros.

A análise das vulnerabilidades identificadas é fundamental para entender a criticidade de cada uma delas, e a pontuação CVSS desempenha um papel crucial nesse processo. Ao todo, foram identificadas 82 vulnerabilidades durante o processo de varredura, com severidades (Alta, Média e Baixa) distribuídas da seguinte forma: 19 Altas (23,17%),

[3]https://cve.mitre.org

33 Médias (40,24%) e 30 Baixas (36,59%). Vulnerabilidades classificadas como altas devem ser tratadas com prioridade máxima, enquanto as de média e baixa severidade podem ser programadas para correção em um cronograma de mitigação a médio/longo prazo. O OpenVAS identifica diversos protocolos de redes para detectar as vulnerabilidades em serviços, incluindo TCP (*Transmission Control Protocol*), UDP (*User Datagram Protocol*) e ICMP (*Internet Control Message Protocol*) para comunicação básica e descoberta de hosts, além de vários protocolos de aplicação, tais como HTTP (*Hypertext Transfer Protocol*), SSH (*Secure Shell*) e RDP (*Remote Desktop Protocol*) [Rahalkar 2018].

Para uma análise mais aprofundada da exposição dos ativos, a Figura 1 apresenta a distribuição das vulnerabilidades identificadas por porta de serviço, segmentadas de acordo com a severidade CVSS. Foram considerados os cinco serviços/portas com maior número de ocorrências, possibilitando uma visualização clara da criticidade associada a cada serviço exposto. Essa abordagem permite visualizar quais serviços estão mais vulneráveis, facilitando a priorização das ações de mitigação em áreas críticas.

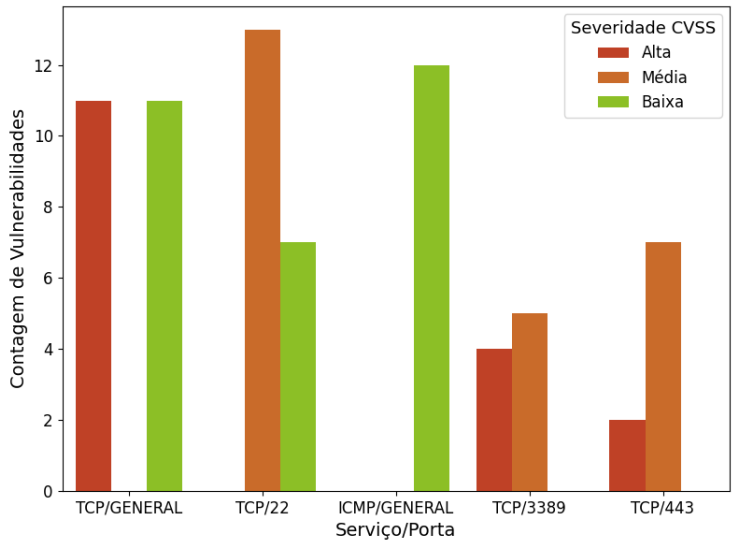

Figura 1. Análise por porta/serviço.

Entre as vulnerabilidades com portas identificadas, destacam-se serviços críticos, como SSH (porta 22), HTTPS (porta 443) e RDP (porta 3389), que devem ser priorizados devido à sua relevância operacional e potencial impacto em caso de exploração. Além disso, vulnerabilidades relacionadas a serviços de rede do Windows, como os protocolos RPC (*Remote Procedure Call*) e SMB (*Server Message Block*), também foram detectadas, reforçando a necessidade de avaliações específicas nessas áreas. Adicionalmente, o OpenVAS pode indicar que algumas ocorrências foram classificadas como "GENERAL", o que significa que a ferramenta não conseguiu determinar diretamente a porta de origem da vulnerabilidade. Nesses casos, é fundamental que a vulnerabilidade reportada seja avaliada no servidor para identificar quais portas estão efetivamente impactadas. Essa distribuição das vulnerabilidades permite direcionar as ações de mitigação para os serviços e portas mais críticos e suscetíveis a ataques, otimizando o uso de recursos e aumentando a eficácia das medidas de segurança implementadas.

A Figura 2 apresenta uma análise conjunta das métricas CVSS e EPSS de um conjunto de vulnerabilidades identificadas, permitindo avaliar de forma mais precisa tanto o impacto potencial quanto a viabilidade de exploração prática de cada vulnerabilidade. Por

exemplo, os CVEs 3, 4 e 5 são muito críticos pois apresentam severidade Alta (CVSS 9.8, 9.3 e 8.8, respectivamente) juntamente com uma alta explorabilidade (EPSS 0.975, 0.795 e 0.968, respectivamente). Por outro lado, a vulnerabilidade representada como CVE 1 apresentou um CVSS de 7,5 (severidade Alta) e um EPSS extremamente baixo (0.001), indicando uma falha tecnicamente severa, mas com baixa probabilidade de exploração no cenário atual. Os CVEs 2 e 6 merecem atenção, pois apesar de terem uma severidade baixa, possuem uma explorabilidade alta, podendo ser estágios iniciais ou intermediários na cadeia de eventos de um ataque cibernético.

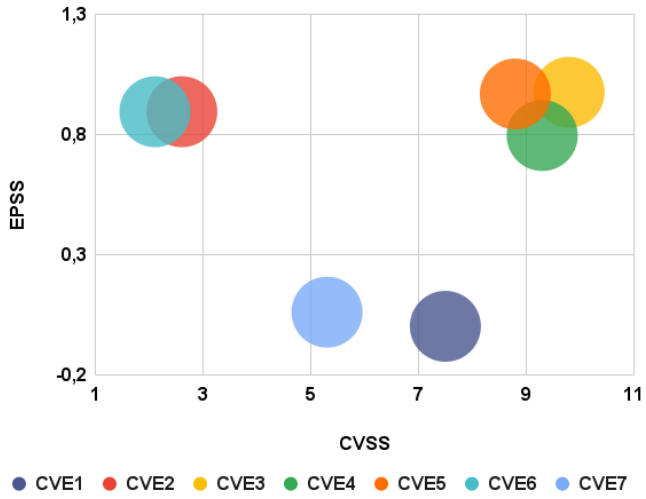

Figura 2. Análise de severidade e explorabilidade.

A Figura 3 apresenta a distribuição da quantidade de vulnerabilidades associadas a cada ativo identificado no ambiente. Este gráfico oferece uma visão clara sobre quais ativos concentram maior número de vulnerabilidades. Nesta análise é importante considerar o tipo e contexto do ativo, por exemplo se ele é um servidor ou uma estação de trabalho comum, se está exposto ou não à Internet, se possui ou não bancos de dados críticos para a organização, etc. Essa análise contextualizada permite uma classificação correta do risco das vulnerabilidades e uma priorização mais assertiva das correções que precisarão ser feitas. Ao analisar essas informações, as equipes de segurança podem direcionar esforços para os ativos mais expostos, otimizando o uso de recursos e reduzindo o risco de comprometimentos críticos na infraestrutura.

Os resultados obtidos evidenciam a eficácia da gestão de vulnerabilidades, integrando severidade (CVSS), explorabilidade (EPSS), existência de *exploits* públicos e contexto do ambiente. Além disso, é válido ressaltar que o estudo alinha-se com boas práticas internacionais de segurança, como o NIST *Cybersecurity Framework* (CSF) e os CIS *Controls* [Bashofi and Salman 2022], ao estruturar um processo de identificação e priorização de vulnerabilidades baseado em métricas de risco e contexto operacional. Com relação ao NIST CSF, têm-se as funções de “Identificar”, “Proteger”e “Detectar”, por meio do mapeamento de ativos, varredura de vulnerabilidades com o OpenVAS e uso de indicadores como CVSS e EPSS. Similarmente, no que se refere ao CIS *Controls*, destacam-se os controles de inventário de ativos, gerenciamento contínuo de vulnerabilidades e verificação da existência de *exploits* públicos. Assim, o trabalho estabelece uma base sólida para a prevenção de ataques cibernéticos e planos de resposta a incidentes mais eficazes, alinhados a *frameworks* amplamente reconhecidos.

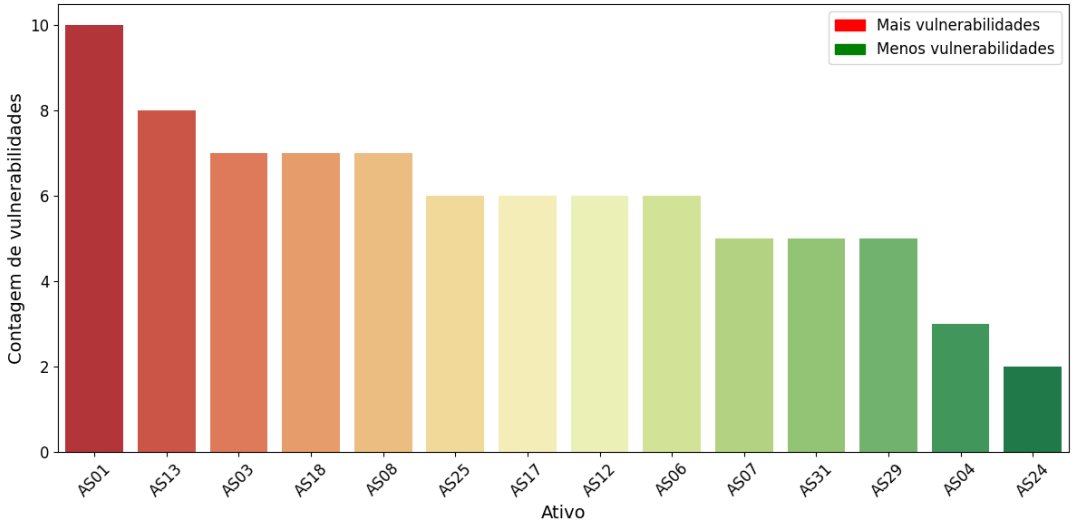

Figura 3. Total de vulnerabilidades por ativo

4. Conclusão

A abordagem apresentada neste trabalho demonstrou potencial para aprimorar a gestão de vulnerabilidades em ambientes computacionais de instituições do setor público com alta diversidade de ativos. Foi possível validar o uso de técnicas de correlação de dados de segurança que vão além da simples detecção de falhas, promovendo uma priorização baseada em risco real, contexto operacional e probabilidade de exploração.

A integração das métricas CVSS, EPSS e a verificação da existência de *exploits* públicos possibilitou uma avaliação mais direcionada e estratégica. Mesmo em uma fase inicial, essa análise multifocal revelou padrões relevantes entre sistemas operacionais, serviços e tipos de vulnerabilidades, indicando o valor da abordagem para apoiar decisões mais eficazes. Como parte dos resultados, relatórios detalhados foram elaborados e entregues à equipe de gestão, descrevendo as principais conclusões de cada análise individual. Esses relatórios incluíram recomendações específicas de mitigação para as vulnerabilidades identificadas, bem como um plano de ação proposto para garantir a continuidade das avaliações de segurança. Esse plano tem como objetivo apoiar a tomada de decisões estratégicas, permitindo que os gestores priorizem questões de alto risco e adotem medidas corretivas imediatas, quando necessário.

Como próximos passos, propõe-se a ampliação do escopo, incluindo varreduras autenticadas, integração com sistemas de resposta automatizada e o uso de modelos preditivos, com o objetivo de fortalecer a resiliência cibernética institucional. Além disso, pretende-se avançar na automatização dos processos de gestão de vulnerabilidades, visando maior eficiência, agilidade para detecção e correção de falhas, visando à redução da dependência de intervenções manuais.

Agradecimentos

Os autores agradecem ao CNPq (Processos 306362/2021-0 e 303877/2021-9) e à SEPLAG/SECITECE/FUNCAP, através do programa Cientista Chefe no projeto ”Testes de Vulnerabilidades e Monitoramento de Segurança Cibernética nos Sistemas Computacionais e Redes de Computadores da SEPLAG”, pelo apoio financeiro.

Referências

Bashofi, I. and Salman, M. (2022). Cybersecurity maturity assessment design using NIST CSF, CIS Controls v8 and ISO/IEC 27002. In *2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom)*, pages 58–62. IEEE.

Center for Internet Security (2023). CIS Critical Security Controls v8. `https://www.cisecurity.org/controls/cis-controls-list`. Accessed: 2025-07-03.

Cruz, D. B., Almeida, J. R., and Oliveira, J. L. (2023). Open source solutions for vulnerability assessment: A comparative analysis. *IEEE Access*, 11:100234–100255.

Ficco, M., Granata, D., Palmieri, F., and Rak, M. (2024). A systematic approach for threat and vulnerability analysis of unmanned aerial vehicles. *Internet of Things*, 26:101180.

FIRST (2019). Forum of Incident Response and Security Teams - Common Vulnerability Scoring System v3.1: Specification Document. Acesso em: 17 maio 2025.

FIRST (2022). Forum of Incident Response and Security Teams - Exploit Prediction Scoring System (EPSS) – v2 Model Documentation. Acesso em: 17 maio 2025.

Liu, Z., Tang, Z., Zhang, J., Xia, X., and Yang, X. (2024). Pre-training by predicting program dependencies for vulnerability analysis tasks. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*, pages 1–13.

National Institute of Standards and Technology (NIST) (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Technical report, NIST. Acesso em: 17 maio 2025.

Offensive Security (2025). Exploit Database (Exploit-DB). Acesso em: 17 maio 2025.

Pimenta, I., Silva, D., Moura, E., Silveira, M., and Gomes, R. L. (2024). Impact of data anonymization in machine learning models. In *Proceedings of the 13th Latin-American Symposium on Dependable and Secure Computing*, LADC '24, page 188–191, New York, NY, USA. Association for Computing Machinery.

Rahalkar, S. (2018). OpenVAS. In *Quick Start Guide to Penetration Testing: With NMAP, OpenVAS and Metasploit*, pages 47–71. Springer.

Rapid7 (2025). Metasploit Framework. Acesso em: 17 maio 2025.

Safitra, M. F., Lubis, M., and Widjajarto, A. (2023). Security vulnerability analysis using penetration testing execution standard (PTES): case study of government's website. In *Proceedings of the 2023 6th international conference on electronics, communications and control engineering*, pages 139–145.

Silva, M., Ribeiro, S., Carvalho, V., Cardoso, F., and Gomes, R. L. (2023). Scalable detection of sql injection in cyber physical systems. In *Proceedings of the 12th Latin-American Symposium on Dependable and Secure Computing*, LADC '23, page 220–225, New York, NY, USA. Association for Computing Machinery.

Thomas, B., Thampi, S. M., and Mukherjee, P. (2025). An in-depth exploration of attack modeling and vulnerability analysis in IoT networks. In *Securing the Connected World: Exploring Emerging Threats and Innovative Solutions*, pages 19–45. Springer.