UTILIZAÇÃO DE TESTES DE PENETRAÇÃO PARA IMPLEMENTAÇÃO E MELHORIAS DA GOVERNANÇA DE TI COM BASE EM SISTEMAS MULTIAGENTES

Palavras-Chave: GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO (TI); TESTES DE PENETRAÇÃO; SISTEMAS MULTIAGENTES.

Autores(as):

HENRIQUE FORTI BALIONI, FATEC AMERICANA

RENATA CALENTE FERNANDES, FATEC AMERICANA

Prof. Dr. JOÃO EMMANUEL D ALKMIN NEVES, FATEC AMERICANA

INTRODUÇÃO:

A crescente complexidade dos ambientes digitais, impulsionada pela rápida evolução dos sistemas computacionais, tem ampliado significativamente a superfície de exposição a ataques cibernéticos. Esses ataques, cada vez mais frequentes e sofisticados, exigem das organizações a adoção de práticas avançadas e integradas no âmbito da Governança de TI (Santos; Moura, 2024). Nesta conjuntura, a Segurança da Informação assume papel fundamental para garantir a confidencialidade, integridade e disponibilidade dos ativos digitais, especialmente diante do aumento das ameaças e da complexidade dos sistemas atuais (Silva, 2024).

Nesse contexto, os Testes de Penetração destacam-se como mecanismo essencial nas análises da postura de segurança organizacional, ao simular ataques controlados que imitam as táticas, técnicas e procedimentos (TTPs) utilizados por agentes maliciosos. Por meio dessa abordagem prática, é possível identificar vulnerabilidades específicas, como falhas em autenticação, configurações incorretas, exposição de dados sensíveis e brechas em aplicações, e operacionais, como permissões excessivas ou falta de segregação de funções. Os Testes de Penetração podem abranger diferentes camadas da Infraestrutura de TI, incluindo redes, sistemas operacionais, aplicações web, APIs, dispositivos móveis e ambientes em nuvem (Silva, 2024).

Apesar da sua importância na identificação de riscos reais, muitas instituições ainda enfrentam desafios para incorporar de forma eficaz os resultados desses testes aos processos decisórios da Governança de TI, especialmente em ambientes complexos que envolvem infraestruturas híbridas, servidores locais, nuvens públicas e privadas, além de dispositivos de Internet das Coisas (Santos; Moura, 2024). Diante dessa limitação, os Sistemas Multiagentes emergem como uma alternativa estratégica, permitindo a modelagem de ambientes computacionais com características autônomas, colaborativas e adaptativas. Esses sistemas são capazes de tomar decisões em tempo real, reagindo

dinamicamente às ameaças cibernéticas e promovendo maior agilidade na detecção e resposta a incidentes (Tonezer *et al*., 2024).

Considerando essa potencialidade, este estudo parte da hipótese de que a integração entre Testes de Penetração e Sistemas Multiagentes pode aprimorar significativamente os processos de Governança de TI, ao fornecer um ambiente dinâmico e simulado para avaliação e resposta a ameaças cibernéticas complexas (Neves *et al*., 2023).

O presente estudo propõe a aplicação integrada dos Testes de Penetração com Sistemas Multiagentes como um recurso inovador para fortalecer a Governança de TI, otimizando os processos de gestão de riscos, segurança da informação e resiliência organizacional. O objetivo geral é desenvolver e validar um ambiente de simulação multiagente para avaliar comportamentos de ataques cibernéticos e respostas defensivas em ambientes controlados (Tonezer *et al*., 2024).

A proposta visa não apenas mapear vulnerabilidades de maneira precisa e contextualizada, mas também propor soluções adaptativas e contínuas frente à atividade das ameaças modernas. Essa abordagem justifica-se pela necessidade crescente de métodos mais sofisticados e automatizados que possam lidar com a complexidade dos ambientes atuais, contribuindo para a melhoria da segurança organizacional e a mitigação eficaz de riscos (Neves *et al*., 2023; Santos; Moura, 2024).

METODOLOGIA:

Este estudo adota uma abordagem exploratória e experimental, fundamentada em revisão bibliográfica e simulação computacional. O desenvolvimento do projeto baseou-se em pesquisas e artigos científicos nas áreas de ameaças cibernéticas, Testes de Penetração, Sistemas Multiagentes e Governança de TI, com o objetivo de analisar comportamentos e respostas diante de ciberataques simulados em ambientes controlados.

A plataforma NetLogo foi selecionada como ferramenta de apoio à modelagem e execução das simulações, devido à sua capacidade de representar sistemas complexos, sua flexibilidade na criação de cenários personalizados e à clareza na visualização das interações entre agentes. O ambiente desenvolvido permite observar, de forma dinâmica, as ações e reações entre componentes simulados de uma infraestrutura de TI sob ataque.

A simulação foi estruturada com foco nas interações entre três categorias de agentes autônomos, organizados de acordo com a metodologia dos Testes de Penetração.

A estrutura organizacional dos agentes no ambiente NetLogo, bem como suas funções operacionais e parâmetros comportamentais, está detalhada na Tabela 1. Essa abordagem permite descrever de forma técnica e objetiva as responsabilidades e capacidades de cada equipe envolvida na simulação (*Red, Blue* e *Purple Team*), conforme os princípios de Testes de Penetração e Governança de TI.

Tabela 1 – Parâmetros dos Agentes no Ambiente Simulado (NetLogo)

Agentes	Função Principal	Comportamento na Simulação
Red Team	Executar ataques simulados como *SQLi, phishing e ransomware*.	Atuam de forma autônoma, escolhendo alvos e tentando comprometer nós vulneráveis com base em capacidade de evasão e frequência de ataque.
Blue Team	Detectar, mitigar e responder a ameaças com estratégias adaptativas.	Monitoram nós vizinhos, identificam comportamentos maliciosos e neutralizam agentes ofensivos, aprimorando ações com base em interações anteriores.
Purple Team	Coordenar os times, analisar dados e propor melhorias de defesa baseadas em boas práticas de Governança de TI.	Realizam auditorias periódicas, identificam padrões emergentes e ajustam estratégias defensivas.

Fonte: Autores (2025)

A simulação foi estruturada com base em uma série de parâmetros configuráveis que determinam o comportamento dos ataques e das defesas durante os ciclos. Cada agente *Red Team* utilizado na simulação representa uma ameaça específica, utilizando técnicas variadas como *SQL Injection* (*SQLi*), *phishing* e *ransomware*.

A probabilidade de sucesso dos ataques varia entre 40% e 80%, dependendo do tipo de ameaça simulada. Esses ataques ocorrem com uma frequência média de 3 ciclos de simulação, sendo que a capacidade de evasão define se o ataque consegue evitar a detecção inicial, podendo ser classificado em baixa, média ou alta.

Quanto à resposta defensiva do *Blue team*, o sistema apresenta um tempo de resposta médio entre 1 a 4 ciclos após a detecção. A capacidade de detecção pode se estender até 2 nós adjacentes, possibilitando a identificação de ameaças em regiões próximas ao ponto de ataque. A simulação considera também uma taxa inicial de falsos positivos de 15%, valor que é ajustado conforme o feedback do sistema. Além disso, o ambiente é analisado a cada 5 ciclos, por meio de auditorias que ajudam a manter a integridade e a vigilância da rede.

No que diz respeito ao *Purple Team* (inteligência do sistema), ele conta com uma capacidade de aprendizado, permitindo que as decisões defensivas melhorem progressivamente após cada processo de mitigação. A coleta de dados é realizada por meio do acesso a logs e informações dos dois times (ataque e defesa), possibilitando inferências e melhorias táticas. Por fim, há uma funcionalidade de atualização estratégica, que propõe ajustes às ações do *Blue Team* com base nas falhas observadas nas execuções anteriores.

Para avaliar o desempenho do ambiente simulado e a eficácia dos agentes frente aos diferentes ataques cibernéticos modelados, foram estabelecidas métricas específicas de avaliação, tanto quantitativas quanto qualitativas. A Tabela 2 apresenta essas métricas, que foram utilizadas para mensurar tempo de resposta, eficácia da defesa, incidência de infecções, entre outros indicadores relevantes.

Tabela 2 – Métricas de Avaliação da Simulação

Métrica	Descrição	Unidade/Tipo
Tempo de detecção	Tempo médio entre o início de um ataque e sua identificação	Inicia com uma média de 12 e evolui até 6 ciclos
Tempo de resposta	Tempo decorrido entre a detecção e a ação defensiva do *Blue Team*	Inicia com 4 ciclos e finaliza com 1 ciclo de simulação
Taxa da infecção	Percentual de nós comprometidos em relação ao total	Aproximadamente 15%
Efetividade de defesa	Número de ataques neutralizados com sucesso	Em média 60% de sucesso na defesa sem os Testes de Penetração; já com os Testes evolui para 85% de efetividade
Taxa de falsos positivos	Incidência de ações defensivas equivocadas (sem ameaça real)	Inicialmente 15%, chegando até em média 5% com a ação dos agentes *Purple*
Crescimento do aprendizado	Redução do tempo de resposta ao longo da simulação	Em média 5 milésimos de segundos a cada ciclo

Fonte: Autores (2025)

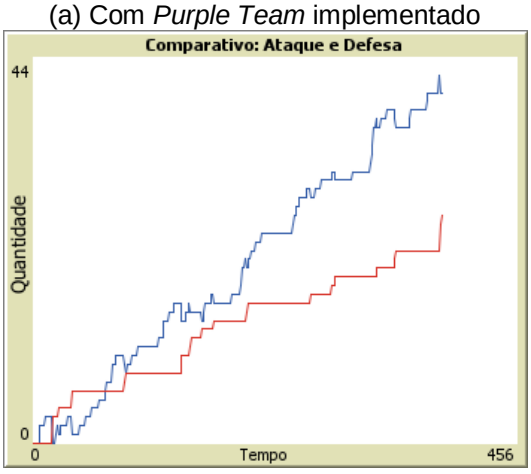
Por fim, ressalta-se que todas as simulações foram feitas em ambiente computacional isolado e controlado, sem contato com sistemas reais ou dados sensíveis, assegurando conformidade com os princípios éticos e legais da pesquisa em Segurança da Informação.

RESULTADOS E DISCUSSÃO:

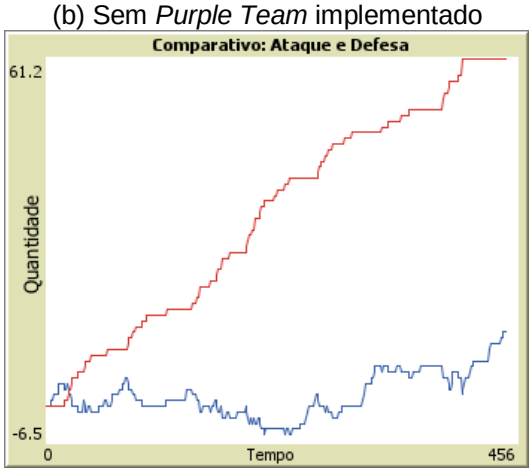
Um dos principais resultados evidenciados foi a constatação de atuação do *Purple Team*, que tem papel decisivo na eficiência do *Blue Team*. As Figuras 1a e 1b demonstram esse impacto, comparando cenários com e sem a presença do *Purple Team*.

Figura 1 – Atuação do *Purple Team* sobre o desempenho do *Blue Team*

(a) Com *Purple Team* implementado



(b) Sem *Purple Team* implementado



Fonte: Autores (2025)

Na Figura 1a, observa-se a implementação do *Purple Team* orientada pelos princípios da Governança de TI e pelo levantamento sistemático de dados. A presença desse agente intermediador favoreceu a conexão efetiva entre as equipes, permitindo identificar vulnerabilidades com maior precisão. Além disso, viabilizou o aprimoramento contínuo das estratégias defensivas, resultando em respostas mais ágeis e eficazes frente aos ataques simulados pelo *Red Team*.

Em contraste, a Figura 1b evidencia um cenário sem a atuação do *Purple Team*. Nesse contexto, houve uma redução significativa na capacidade de mitigação do *Blue Team*, revelando falhas no planejamento e na execução das defesas. Esse resultado reforça a importância da Governança de TI integrada como elemento estratégico para fortalecer a segurança da informação, especialmente em contextos baseados em Testes de Penetração.

Deste modo, a simulação demonstrou que ações colaborativas entre agentes reforçam a detecção e mitigação de ameaças, ampliando a segurança em ambientes complexos.

CONCLUSÕES:

Com base na pesquisa e nos dados levantados, conclui-se que a implementação da Governança de TI, com normas práticas e técnicas avançadas, é essencial para viabilizar Testes de Penetração periódicos nas instituições. A aplicação de Sistemas Multiagentes, representada pela ferramenta NetLogo, demonstrou-se eficiente ao simular o comportamento dos agentes em diferentes cenários e equipes. Essa abordagem permitiu analisar interações de ataque, detecção e cooperação, evidenciando ações adaptativas que fortalecem a maturidade, resiliência e segurança dos sistemas, alinhadas à Governança de TI.

BIBLIOGRAFIA

NEVES, J. E. D. A.; PEDRO, P. S. M.; HERNANDEZ, M. F. G.; FABRI JUNIOR, L. A. **Simulation of the Implementation of Domestic Solar Systems Using Multi-agent Systems from Web Scraping**. Smart Innovation, Systems and Technologies. 1ed.: Springer International Publishing, 2023, v. 1, p. 88-96. Disponível em: https://doi.org/10.1007/978-3-031-04435-9_8. Acesso em: 16 maio 2025.

SANTOS, V. M. S.; MOURA, L. F. **Características Essenciais da Governança de TI**: Uma Revisão Sistemática de Literatura. Ponta Grossa, 2024. Disponível em: https://admpg.com.br/2024/anais/arquivos/07272024_140741_66a531cdc1aae.pdf. Acesso em: 16 maio 2025.

SILVA, L. P. O. **Pentest Baseado em Imagens Encase**: Uma Análise de Vulnerabilidades em Servidores Web. Goiânia, 2024. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/8086. Acesso em: 16 maio 2025.

TONEZER, L. N.; SILVA, A. C. M.; ALMEIDA, A. H.; NEVES, J. E. D. **Simulações Multiagentes e Phishing**: Explorando a Segurança em Ambientes de Nuvem. Americana, Revista Tecnológica da Fatec de Americana, v. 11, n. 2, 2024. Disponível em: https://fatec.edu.br/revista/index.php/RTecFatecAM/article/view/393. Acesso em: 16 maio 2025.