A INFLUÊNCIA DO USO DAS METODOLOGIAS SEGUNDO PENTESTERS:
UM ESTUDO QUALIQUANTITATIVO\ DO USO DAS DIFERENTES METODOLOGIAS DE PENTEST

Arthur Ribeiro Guirro(a)[1]

Guilherme Corredato Guerino(a)[2]

RESUMO

A proteção de dados se tornou uma prioridade devido ao aumento de ataques cibernéticos, e o Teste de Penetração (Pentest) é uma prática essencial para identificar e corrigir vulnerabilidades. Este estudo tem como objetivo analisar as metodologias de pentest utilizadas por profissionais da área, por meio de uma pesquisa com questionários aplicados a especialistas em segurança ofensiva. A pesquisa adota a metodologia de survey e coleta dados de 16 profissionais com experiência em Pentests. O questionário foi dividido em quatro seções: dados pessoais, uso das metodologias, aplicação prática e uso de inteligência artificial. Os resultados indicam que metodologias consolidadas como OWASP, PTES e NIST são amplamente adotadas, com algumas adaptações conforme as necessidades dos clientes. As ferramentas Nmap e Burp Suite foram destacadas como essenciais para a identificação de vulnerabilidades. Os profissionais enfatizam a importância do planejamento e da definição do escopo, com flexibilidade nas etapas do pentest, adaptando-as conforme o contexto do teste. A inteligência artificial (IA) foi mencionada como uma ferramenta útil, mas com limitações, sendo vista como complementar ao trabalho humano. A conclusão destaca a relevância das metodologias padronizadas, a personalização dos testes e a necessidade de uma comunicação clara com os clientes.

PALAVRAS-CHAVE: Segurança ofensiva; Vulnerabilidades; Teste de Penetração.

INTRODUÇÃO

A sociedade, ao longo da história, tem enfrentado conflitos relacionados à busca por bens, informações e à autopreservação. Com o avanço da tecnologia, esses conflitos adquiriram novas formas, especialmente no que tange à proteção de dados, que se tornaram uma prioridade para empresas. O uso indevido de informações pode causar grandes prejuízos financeiros, e as vulnerabilidades tecnológicas expõem dados sensíveis a ataques. De acordo com a IBM, “os testes de penetração podem ajudar as empresas a comprovar a conformidade com esses regulamentos, garantindo que seus controles funcionem conforme o pretendido.”

1 Universidade Estadual do Paraná, arthurguirro@gmail.com.
2 Universidade Estadual do Paraná, guilherme.guerino@ies.unespar.edu.br.

Essa realidade exige a implementação de medidas para proteger os dados, como o Teste de Penetração (Pentest), que simula ataques em sistemas para identificar e corrigir vulnerabilidades.

O Pentest é uma invasão ética, realizada por especialistas para testar a robustez e confiabilidade dos sistemas, com o objetivo de garantir sua segurança. Ele é essencial para proteger dados, tanto fisicamente quanto virtualmente, empregando técnicas que dificultam acessos não autorizados. A invasão pode ocorrer de diversas formas, dependendo do escopo definido pela empresa, e a padronização dos testes se tornou necessária para assegurar a confiabilidade dos resultados. Nesse contexto, a utilização de metodologias de pentest desempenha um papel crucial, estabelecendo diretrizes e procedimentos para os testes, o que facilita tanto para os profissionais que executam os testes quanto para as empresas contratantes.

Com a crescente variedade de metodologias disponíveis, a escolha da abordagem adequada para cada situação se tornou uma tarefa desafiadora. O processo de execução de um Pentest segue métricas para manter a confiabilidade, sendo a padronização essencial para orientar o trabalho dos especialistas. A execução padronizada busca apoio por meio de guias e melhores práticas, mas, devido à diversidade de possibilidades, a padronização pode ser uma tarefa complexa (KNOWLES et al., 2016). A análise crítica dessas metodologias é necessária para determinar quais são mais eficazes, levando em conta seu uso diário e as peculiaridades de cada ambiente.

Este trabalho visa identificar padrões nas metodologias de pentest utilizadas por profissionais da área, com uma análise quantitativa e qualitativa baseada em questionários aplicados a especialistas. Os objetivos específicos incluem comparar o uso das metodologias em ambientes comerciais, analisar sua influência nos processos de pentest e na apresentação de resultados, além de explorar a percepção dos profissionais em relação às etapas e processos envolvidos nos testes de penetração.

METODOLOGIA

Este estudo adotou o método de pesquisa do tipo survey, com foco em profissionais da área de segurança ofensiva e com experiência prática em Pentests. O objetivo principal foi coletar dados que refletissem o uso das metodologias de Pentest no mercado, proporcionando uma análise crítica sobre a aplicação teórica e prática dessas abordagens. Para garantir a

qualidade dos dados coletados, foi realizado um survey piloto, validado por especialistas da área e pesquisadores, ajustando as questões do questionário de acordo com os desafios reais enfrentados pelos profissionais. O questionário final, composto por 22 questões abertas, foi dividido em quatro seções: dados pessoais, utilização das metodologias, aplicação prática e uso de inteligência artificial (IA) nos Pentests.

O survey foi disponibilizado online através da plataforma Google Forms, de 07/10/2024 a 27/10/2024, e divulgado via LinkedIn, atingindo diretamente os profissionais da área. Durante esse período, foram obtidas 16 respostas, que formaram a base da análise dos dados. A escolha do LinkedIn como meio de divulgação foi estratégica para atingir um público qualificado, garantindo que os participantes tivessem experiência relevante em Pentests. Todos os participantes foram informados sobre os objetivos da pesquisa e sobre o uso anônimo dos dados coletados, assegurando a adesão voluntária e a ética no processo.

A análise dos dados foi realizada com o apoio das ferramentas WPS Office 2019 e Flourish. O WPS Office foi utilizado para organizar e tabular as respostas qualitativas e quantitativas, enquanto o Flourish possibilitou a criação de visualizações gráficas, facilitando a interpretação dos dados. A combinação dessas ferramentas permitiu uma análise detalhada das respostas, considerando tanto aspectos demográficos quanto as percepções dos participantes sobre o uso das metodologias de Pentest e a introdução da IA no processo.

Os materiais utilizados neste estudo incluem o questionário do survey, que pode ser consultado no Apêndice B, e o Termo de Consentimento Livre e Esclarecido (TCLE), presente no Apêndice A. Esses documentos foram elaborados em conformidade com as normas éticas e metodológicas, garantindo a confiabilidade e validade dos dados. A metodologia empregada, portanto, seguiu rigorosamente as práticas recomendadas para garantir a precisão e a ética na coleta e análise das informações.

RESULTADOS E DISCUSSÕES

Os dados obtidos durante a aplicação do questionário revelam uma diversidade significativa entre os participantes, que vêm de diferentes localidades, tanto do Brasil quanto do exterior, com predominância do estado de São Paulo. As faixas etárias variam de 18 a 48 anos, com maior concentração entre 18 e 25 anos. A experiência dos participantes na área de pentest varia de 1 a 8 anos, sendo que a maioria possui entre 4 e 6 anos de experiência. A maioria dedicou de 1 a 5 anos ao estudo de segurança ofensiva.

Em relação à área de atuação profissional, a pesquisa mostrou que a maior parte dos participantes trabalha com pentest em aplicações web, seguido de aplicações mobile. Também foram mencionadas outras áreas, como pentest em redes wireless, sistemas operacionais e infraestruturas. Essas informações refletem uma ampla gama de experiências e especializações dentro da área de pentest.

O estudo sobre a aplicação de metodologias de pentest mostrou grande diversidade nas abordagens utilizadas. A maioria segue metodologias consolidadas, como a OWASP, especialmente em testes de aplicações web, mas também é comum o uso de metodologias próprias adaptadas pelas empresas. Como um dos participantes destacou: "a empresa costuma adaptar essas metodologias para atender melhor às necessidades específicas de cada cliente". Isso reflete uma tendência de personalização das metodologias para alcançar melhores resultados em cenários específicos, combinando práticas amplamente aceitas, como PTES e NIST, com ajustes internos.

Quanto às etapas do pentest, os participantes destacaram a importância do planejamento e da definição do escopo para alinhar expectativas entre o cliente e o pentester, como exemplificado pelo Participante 2:

- *"defino com o cliente os objetivos do teste, o escopo exato, o nível de conhecimento fornecido e as restrições operacionais".*

A coleta de informações e a análise de vulnerabilidades também foram consideradas essenciais para a realização de testes eficazes. Ferramentas como Nmap e Burp Suite foram citadas como indispensáveis para identificar falhas, enquanto a exploração das vulnerabilidades foi vista como a etapa crucial para avaliar o impacto real das falhas.

Apesar de a maioria dos profissionais reconhecer que todas as etapas são interdependentes, alguns participantes observaram que, em contextos específicos, certas fases podem ser menos importantes. Por exemplo, a fase de pós-exploração foi considerada menos crítica quando o objetivo é apenas identificar vulnerabilidades, sem necessidade de uma exploração profunda, como comentou o Participante 6:

- *"quando o objetivo principal é identificar vulnerabilidades, a análise de movimento lateral e a persistência podem ser menos críticas".*

Essas variações demonstram a flexibilidade das metodologias de pentest, que podem ser ajustadas conforme os objetivos e o escopo do teste.

O processo de pentest, conforme descrito pelos participantes, inicia com uma reunião com o cliente para definir expectativas e escopo. Em seguida, são planejadas as etapas de reconhecimento, enumeração, exploração de vulnerabilidades e pós-exploração, sempre com base em metodologias estabelecidas como PTES, OWASP e Cyber Kill Chain. Essas metodologias garantem qualidade e organização no processo, e os participantes enfatizam a importância do planejamento inicial, incluindo a definição de escopo e formalização do serviço.

A execução das etapas técnicas envolve o uso de ferramentas como OSINT, escaneamento de redes e exploração de vulnerabilidades conhecidas. Os participantes destacam a importância de um relatório final claro e detalhado, que permita aos gestores entender o impacto das vulnerabilidades encontradas e tomar medidas corretivas adequadas. A integração entre teoria e prática é ressaltada, mostrando como as metodologias ajudam a estruturar o processo, mas que a flexibilidade é necessária para adaptar os testes às particularidades de cada projeto.

O prazo para a realização dos pentests varia conforme a complexidade do escopo e os ativos a serem testados. A maioria dos participantes destaca que o tempo pode ser ajustado, especialmente em casos de mudanças no escopo ou imprevistos. O prazo médio para testes simples, como os de aplicações web e mobile, é de 1 a 2 semanas, enquanto testes mais complexos, como os de infraestrutura e cloud, podem levar de 2 a 3 semanas.

A estruturação do relatório final é crucial. Os participantes mencionam que ele deve ser acessível tanto para o público técnico quanto para o executivo, contendo um resumo executivo, a descrição do escopo e metodologia, e um detalhamento das vulnerabilidades encontradas e suas implicações. A organização das vulnerabilidades segue uma classificação de severidade, incluindo recomendações práticas para mitigação. A utilização de metodologias padronizadas como PTES, OWASP e OSSTMM é importante para reforçar a credibilidade do processo e garantir a qualidade das análises. A comunicação com o cliente é essencial para alinhar expectativas, especialmente quanto ao prazo e à entrega do relatório, garantindo que qualquer alteração seja acordada de forma transparente e eficaz.

O uso da inteligência artificial (IA) na segurança ofensiva gerou discussões sobre seu impacto e eficácia. Os participantes destacaram que a IA é uma ferramenta valiosa, especialmente em tarefas repetitivas, como automação na detecção de ataques zero-day e na redação de relatórios, aumentando a eficiência. Contudo, muitos ressaltaram que a IA ainda

não consegue atingir o nível de precisão exigido em atividades mais complexas, como testes de penetração detalhados. A IA é vista como uma extensão do trabalho humano, eficaz na organização de grandes volumes de dados e na detecção de padrões, mas sempre necessitando da validação de um analista humano para garantir a confiabilidade dos resultados.

Quando questionados sobre a possibilidade de substituir completamente a inteligência humana em um pentest, a resposta predominante foi negativa. Diversos participantes enfatizaram que, embora a IA seja útil na automação de tarefas repetitivas e na análise de vulnerabilidades, ela não possui a criatividade e o pensamento crítico necessários para lidar com cenários não convencionais ou sofisticados. Como afirmou o participante 5:

- *"A criatividade humana não pode ser superada por uma inteligência artificial".*

Portanto, a IA é vista como uma ferramenta auxiliar, mas não capaz de substituir a expertise e o julgamento humano, essenciais para o sucesso do pentest.

No cenário atual, a IA é considerada uma aliada poderosa, mas com limitações, principalmente em tarefas complexas que exigem julgamento humano. O uso de IA, como a tecnologia XBOW, demonstrou que a automação de pentests pode ser eficiente, realizando testes com rapidez e precisão comparáveis aos dos profissionais humanos. Contudo, a IA ainda enfrenta dificuldades em tarefas que exigem criatividade e intuição, elementos que os profissionais humanos trazem para o processo. Como o especialista Federico Muttis mencionou, a IA complementa, mas não substitui os pentesters humanos, sendo mais eficaz como uma ferramenta que trabalha em conjunto com o conhecimento humano.

CONCLUSÃO

Este estudo investiga o uso de metodologias de pentest em cenários reais, com foco nas práticas adotadas por profissionais da segurança ofensiva. Os resultados revelam que as metodologias mais consolidadas, como OWASP, PTES e NIST, são amplamente utilizadas, com algumas adaptações personalizadas para atender às necessidades específicas de cada cliente. As metodologias orientam o processo de pentest, proporcionando consistência e clareza nos testes realizados. A aplicação de ferramentas como Nmap e Burp Suite, destacadas pelos participantes, é essencial para a identificação de vulnerabilidades. A flexibilidade nas etapas do pentest, adaptando-as ao escopo do teste, também é importante para garantir a eficácia dos resultados. A análise das respostas confirma a relevância das metodologias na definição do escopo, planejamento e execução dos testes. O uso de IA,

embora útil, é visto como uma ferramenta complementar, não substituindo o julgamento humano nas tarefas mais complexas. Os profissionais reconhecem a importância da personalização das metodologias, mas mantêm os padrões para garantir a qualidade dos testes. A comunicação clara com os clientes é fundamental para o sucesso dos pentests. Em futuro, sugere-se um estudo mais aprofundado sobre a aplicação da IA na segurança ofensiva.

REFERÊNCIAS

IBM. O que é o teste de penetração? Disponível em: https://www.ibm.com/br-pt/topics/penetration-testing. Acesso em: 14 out. 2024.

KNOWLES, W.; BARON, A.; MCGARR, T. The simulated security assessment ecosystem: Does penetration testing need standardisation? Computers & Security, v. 62, set. 2016. Disponível em: https://www.researchgate.net/publication/306078206_The_simulated_security_assessment_ecosystem_Does_penetration_testing_need_standardisation. Acesso em: 15 nov. 2024.

MOOR, Oege de. XBOW: Entrar na lista de espera. 2024. Disponível em: https://xbow.com. Acesso em: 14 out. 2024.