

## Identificação do perfil de *pentester* desejado pelas empresas brasileiras

Leonardo Tobias – Centro Federal de Educação Tecnológica de Minas Gerais  
leonardobotrel@gmail.com

<https://orcid.org/0009-0008-3893-8340>

Mateus Tymburibá – Centro Federal de Educação Tecnológica de Minas Gerais

<https://orcid.org/0000-0002-6626-1786>

mateustymbu@gmail.com

---

**Resumo** – A segurança computacional tem evoluído de maneira tão rápida que tem sido difícil identificar os principais requisitos exigidos para profissionais dessa área. Este estudo identifica as competências mais importantes para execução de testes de penetração em sistemas computacionais. As soluções atuais para o mapeamento das características desejáveis de um *pentester* são limitadas. Este trabalho propõe uma solução automatizada para coletar e classificar essas características. A relevância dos requisitos coletados é estabelecida com base na menção, na influência e na importância de cada competência identificada. Os resultados mostram que as empresas brasileiras preferem profissionais certificados, com domínio de redes e especializados em aplicações móveis ou em sistemas web. Fluência em inglês também é essencial.

**Palavras-chave:** *pentest*, teste de penetração, requisitos, competências, habilidades

---

## Identification of the *pentester* profile desired by Brazilian companies

**Abstract** – The field of computer security has been evolving so rapidly that it has been difficult to identify the main requirements demanded of professionals in this area. This study identifies the most important skills for conducting penetration tests on computer systems. Current solutions for mapping the desirable characteristics of a *pentester* are limited. This work proposes an automated solution for collecting and classifying these characteristics. The relevance of the collected requirements is established based on the mention, influence, and importance of each identified competency. The results show that Brazilian companies prefer certified professionals with expertise in networks and specialization in mobile applications or web systems. Fluency in English is also essential.

**Keywords:** *pentest*, penetration testing, requirements, skills, abilities

---

**Data da Submissão:** 12/08/2023

**Data de aceitação:** 18/12/2023

Agradecemos ao CEFET-MG pelo apoio durante o desenvolvimento deste trabalho.

Este artigo está licenciado sob forma de uma licença Creative Commons Atribuição-Não Comercial-Sem Derivações 4.0 Internacional (CC BY-NC-ND 4.0).

<https://creativecommons.org/licenses/by-nc-nd/4.0/>



DOI: <https://doi.org/10.51359/2317-0115.2023.260729>

## 1. Introdução

As tendências globais do mercado de trabalho estão mudando rapidamente devido ao desenvolvimento ativo das tecnologias digitais. A automação e o desenvolvimento de inovações tecnológicas levaram à disseminação de tecnologias de realidade aumentada (APEAGYEI, 2019), robótica (BISWAS, 2018), Internet das Coisas (WORTMANN, 2015), finanças digitais, serviços (GABOR, 2017) e a transformação digital de setores inteiros da economia (BOKOLO, 2021). Ao mesmo tempo, de acordo com um estudo realizado pelo Cetic.br (CETIC, 2020), a pandemia de COVID-19 intensificou o uso de tecnologias digitais no Brasil, passando de 71% dos domicílios com acesso à internet em 2019 para 83% em 2020. Outra pesquisa, realizada pela Fundação Getúlio Vargas (FGV, 2022), mostrou que a pandemia acelerou o processo de transformação digital das empresas no Brasil. Todo esse incremento digital veio acompanhado de uma elevação dos riscos de segurança. Uma reportagem do Estadão (ESTADAO, 2022) afirma que o noticiário de *cibersegurança* está aquecido, com muitos relatos de ataques a empresas do Brasil e do mundo, fato que levou a uma demanda maior por especialistas da área, inclusive com um consequente aumento do salário médio da categoria. Além disso, o Consórcio Internacional de Certificação de Segurança de Sistemas de Informação (ISC2, 2022) revelou que em 2022 havia um déficit global de 3,4 milhões de especialistas em *cibersegurança*. Como consequência, a demanda por especialistas nessa área segue elevada.

Um capital humano altamente qualificado é pré-requisito para o desenvolvimento das empresas e da economia como um todo (GIORDANO, 2013). Em particular, existe uma grande demanda pelo desenvolvimento de habilidades específicas relacionadas a *pentesters* - profissionais que atuam com testes de penetração em sistemas computacionais, a fim de encontrar vulnerabilidades e corrigi-las para elevar sua segurança. No entanto, pode ser um desafio encontrar pessoas com competências de alta qualidade, especialmente entre aqueles que estão ingressando na área ou ainda estão no ambiente educacional, devido à alta velocidade do desenvolvimento tecnológico. Portanto, é essencial o desenvolvimento de soluções que avaliem e prevejam a necessidade de especialistas devidamente qualificados (HOSU, 2016). Assim, minimizar as diferenças entre a demanda por esses requisitos e sua oferta é fundamental. Este trabalho visa identificar a estrutura de competências da profissão de *pentester* no Brasil.

Para isso, foi usado um *Web Scraper* (ferramenta usada para coletar informações em sites) para registrar automaticamente o conteúdo de vagas de emprego disponíveis na plataforma do LinkedIn®. Em seguida, foi feita uma identificação manual das competências buscadas por empresas em *pentesters*, com base no conteúdo das vagas, que então foram classificadas em categorias em uma identificação manual de qual área da computação cada requisito faz parte. Essas competências foram então classificadas em relação à frequência em que são mencionadas nas vagas de emprego (análise da frequência de menção). Essa separação mostra quais são os requisitos mais exigidos.

Além da distinção por frequência de aparição dos requisitos, foi construída uma rede de relacionamentos bidirecionais entre essas competências. Essa rede foi definida com base na aparição conjunta de habilidades nas vagas de emprego. Ou seja, se um requisito aparece junto com outro em uma mesma vaga, considera-se que eles estão relacionados e cria-se uma ligação entre eles na rede. Foi usado um peso para essas ligações equivalente à quantidade de vezes em que uma determinada relação ocorreu. Essa rede de relacionamentos foi importada para o Gephi® (pacote de *software* usado para

análise de redes e grafos) (CHERVEN), a fim de se visualizar quais são as competências mais influentes e o quão fortemente uma habilidade está ligada a outras (análise da influência e correlação entre as competências). Dessa forma, é possível estabelecer quais requisitos devem ser aprendidos em conjunto. Por fim, essa rede de relacionamentos foi classificada de acordo com o algoritmo *PageRank* (algoritmo que mede a importância de um nó em uma rede), gerando um *ranking* com as competências mais importantes, como forma de complementar a classificação em relação à frequência de ocorrência dos requisitos.

Os resultados mostraram que requisitos relacionados à área de redes de computadores são mencionados com mais frequência, enquanto habilidades gerenciais - como engenharia de software e gerenciamento de projetos - dificilmente aparecem em vagas de emprego para *pentesters*. Apesar desse esperado viés técnico das vagas oferecidas para segurança ofensiva de *software*, há também resultados surpreendentes, como a baixa menção a tipos clássicos de vulnerabilidades de *software*, como XSS, CSRF e injeção SQL. Destacaram-se também o peso de certificações para alavancar candidaturas a uma vaga de *pentester*, além da exigência de proficiência na língua inglesa.

Quando comparado a trabalhos relacionados, o modelo de priorização de competências desenvolvido neste trabalho utiliza um número maior de estratégias para classificar os requisitos, gerando uma análise mais completa e potencialmente mais precisa. Além disso, até onde se tem conhecimento, é o primeiro estudo focado em compreender o perfil desejado do profissional especialista em testes de invasão de sistemas computacionais.

Do ponto de vista da comunidade de segurança de software brasileira, com posse desses resultados, fica mais simples estabelecer quais competências são mais relevantes para as empresas que estão buscando profissionais na área. Dessa forma, tanto pessoas que querem iniciar na carreira e precisam saber por onde começar a estudar, quanto profissionais experientes que estão em constante aprimoramento e necessitam saber onde investir esforços para evolução, podem se beneficiar deste trabalho. Instituições de ensino também podem encontrar nesses resultados uma base fundamentada para a elaboração de cursos e planos de ensino.

## 2. Trabalhos relacionados

A identificação das competências exigidas pelo mercado de trabalho para pessoas que estão iniciando uma carreira é uma área de pesquisa popular (GOLDSMITH, 1994). A definição do perfil profissional para uma determinada posição pode ser baseada na análise de anúncios de emprego em *sites* ou plataformas *online* (CALANCA, 2019). Esses anúncios de contratação refletem a visão do empregador sobre o candidato ideal. Essa abordagem desempenha um papel importante na definição dos requisitos para um cargo específico, embora apenas alguns desses requisitos sejam efetivamente considerados durante o processo de recrutamento (GARDINER, 2018). Nesse sentido, os portais de emprego online podem ser ferramentas úteis para determinar o perfil desejado dos profissionais.

No Brasil, existem poucos estudos que buscam identificar o perfil de um profissional. Em um desses projetos, os autores focaram nos requisitos exigidos pelo mercado de trabalho para profissionais da área contábil na região norte do Brasil (TAMER, 2013). O método utilizado consistiu em avaliar a frequência de menção dos

requisitos nos anúncios de emprego. Os resultados sugeriram que o profissional mais desejado pelo mercado é aquele que possui conhecimentos operacionais, com menos ênfase em habilidades de tomada de decisão.

Tonelli (2019) traçou o perfil do profissional da controladoria requisitado pelas empresas brasileiras. Para isso, os anúncios de emprego foram coletados manualmente, e também foi utilizada a frequência de menção dos requisitos para avaliação. A autora identificou que os requisitos mais solicitados nos anúncios são: elaboração e interpretação de relatórios, análise e avaliação econômica, controle e planejamento, além de habilidades na área contábil.

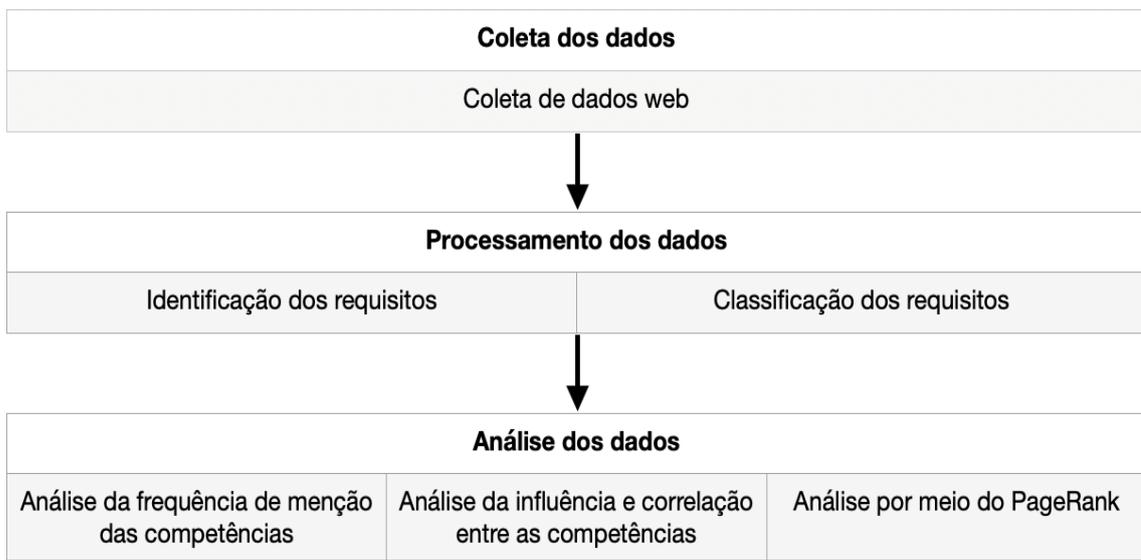
Por fim, Dutra avaliou as habilidades exigidas pelo mercado de trabalho para os profissionais de tecnologia da informação (DUTRA, 2006). A autora coletou os dados manualmente em sites de emprego e realizou pesquisas bibliográficas. A frequência de menção dos requisitos foi usada para analisar as tendências do mercado na definição das habilidades buscadas nos profissionais. O estudo concluiu que as habilidades exigidas para os profissionais de TI incluem conhecimentos técnicos, fluência em idiomas estrangeiros, domínio de informática, conhecimentos gerenciais e, principalmente, habilidades interpessoais.

A maioria dos estudos relacionados (TAMER, 2013; TONELLI, 2019) não aborda especificamente a área de profissionais de TI e, quando o fazem (DUTRA, 2006), não focam especificamente em profissionais de *pentest*. Além disso, esses estudos geralmente realizam a coleta de informações e análise de dados de forma manual, utilizando apenas a análise da frequência de menção das competências nos anúncios de emprego. Portanto, este estudo se diferencia dos demais ao adotar uma coleta automatizada de dados. O processo de geração da frequência de menção também é automatizado. Além disso, este estudo apresenta a correlação entre as habilidades por meio de uma rede de relacionamentos, destacando a importância de cada aptidão nessa rede.

### 3. Competências prioritárias

Neste estudo, a coleta e a análise de dados foram realizadas em três etapas, conforme ilustrado na figura 1. Na primeira etapa, os dados foram coletados automaticamente por meio do *web scraping* (varredura web), utilizando o *site* do LinkedIn® como fonte de vagas para *pentesters*. O LinkedIn®, pertencente à *Microsoft*, é a maior rede profissional do mundo, com mais de 774 milhões de usuários em mais de 200 países e territórios em 2022. Foram realizadas pesquisas no *site* utilizando as seguintes expressões: *pentester*, *pentest* e *analista de segurança*. Os *links* com os resultados dessas pesquisas foram inseridos em um programa escrito em Ruby®. O programa percorreu cada vaga retornada em cada pesquisa, coletou as informações de seu conteúdo e as salvou em um banco de dados. O processo de coleta de dados foi facilitado pelo uso da API Kimurai, uma ferramenta que extrai informações de *sites* e está disponível como um pacote Ruby (KIMURAI, 2023). Foi coletado um total de 207 anúncios de emprego.

Figura 1 – Etapas de coleta e análise dos dados.



Na segunda etapa, o conteúdo de cada vaga foi analisado manualmente, removendo postagens repetidas ou que não se enquadravam como oportunidades para profissionais de *pentest*. A amostra resultante consistiu em 127 vagas de trabalho, distribuídas por todo o Brasil, com propostas de trabalho presencial e remoto. A maioria das empresas que publicaram os anúncios eram médias e grandes instituições, principalmente do setor de tecnologia e bancário. Durante esse processo de análise, cada aptidão identificada nas vagas foi registrada. Como resultado, foram elencadas 104 habilidades relacionadas ao trabalho de um *pentester*. Devido à quantidade considerável de competências, elas foram divididas em 14 categorias para facilitar a compreensão deste estudo. Essas classes foram selecionadas por meio de pesquisa manual para determinar a área de conhecimento à qual cada habilidade estava relacionada, resultando nas seguintes categorias.

Quadro 1 - Habilidades usualmente requeridas ao *pentester* e suas respectivas categorias neste estudo.

Domínio Técnico	Conhecimento Aplicado	Capacitações	Competências Sociais
Sistemas operacionais	Redes de computadores	Certificações	Habilidades comportamentais
Linguagens de programação	Segurança de redes e seus aspectos computacionais	Gerenciamento de Projetos	Habilidades de comunicação
Domínio de <i>software</i>	Computação em nuvem	Em leis e normas de segurança	Envolvimento com a comunidade
Engenharia de <i>software</i>	Conhecimento de vulnerabilidades		

Fonte: GitHub deste trabalho (PENTESTER, 2023).

Na terceira e última etapa, as competências foram classificadas com o uso de três técnicas diferentes: a frequência de menção, a influência e correlação entre as aptidões, e com o uso do algoritmo *PageRank*. A classificação da frequência de menção foi feita com o auxílio de um algoritmo que percorreu cada vaga e contabilizou quantas vezes cada habilidade foi mencionada.

Dessa forma, foi possível identificar quais competências são mais frequentemente demandadas nas oportunidades de emprego e quais não são. Em seguida, foi construída uma rede de interação bidirecional entre os diferentes requisitos profissionais, onde cada habilidade mencionada em uma vaga junto com outra habilidade entrou nessa rede como uma ligação. A cada vez que uma correlação específica aparecia, ou seja, quando uma combinação de habilidades ocorria em uma vaga, era atribuído um valor a essa combinação, denominado peso, que indica a força dessa correlação.

Por exemplo, OSSTMM (Open Source Security Testing Methodology Manual ou Manual de Metodologia de Teste de Segurança de Código Aberto, em tradução livre) e Red Team (equipe responsável por simular um *ciberataque* contra uma empresa) (REDTEAM, 2023) são habilidades que apareceram juntas em 30 vagas. Portanto, o peso da conexão entre elas é 30. Quanto maior o peso, maior a correlação entre uma habilidade e outra. Essa rede de relacionamento foi importada para o Gephi (CHERVEN, 2013). Em seguida, foram utilizadas rotinas do Gephi para exibir visualmente e de maneira clara a influência que uma aptidão possui sobre outra. Dessa forma, um profissional pode determinar quais habilidades são mais relevantes para serem desenvolvidas em conjunto. Retomando o exemplo mencionado anteriormente, se um profissional tem interesse em aprender Red Team, talvez seja benéfico também adquirir conhecimentos em OSSTMM. A análise abrangeu 4.392 pares de habilidades.

Por fim, utilizou-se o algoritmo PageRank (BRIN, 2012) para validar a importância de habilidades estabelecida através do método de contagem da frequência de menções. PageRank é o famoso algoritmo criado pelos fundadores do buscador Google para ordenar as páginas exibidas no resultado de uma consulta segundo um critério de importância melhor do que a contagem de aparições das expressões buscadas. Nesse algoritmo, a importância de um nó (página web) é determinada pela quantidade e pela qualidade de outros nós que apontam para esse nó específico da rede. Neste estudo, o PageRank foi empregado para classificar a rede de habilidades criada na etapa de análise de influência. Para o PageRank, uma competência é considerada importante se ela estiver ligada a uma outra habilidade importante, ou se ela estiver conectada a muitas competências. Tendo em vista o processo de cálculo iterativo adotado pelo PageRank, em que a relevância inicial de cada nó da rede é inicializada com um valor padrão, essa análise não considerou o peso das conexões entre competências, apenas a sua existência. Por meio do PageRank, foi possível determinar, através de um segundo método, quais aptidões são mais relevantes e devem ser desenvolvidas prioritariamente.

#### 4. Resultados

O presente estudo buscou obter resultados a partir do uso de três técnicas distintas: análise de frequência, análise de influência e correlação e análise via PageRank. A análise de menção e a análise por meio do PageRank tiveram como foco identificar quais são as competências mais demandadas e importantes para o profissional de *pentest*, agindo de maneira complementar para garantir maior confiabilidade aos resultados. A análise de influência e correlação, por sua vez, objetivou identificar quais competências devem ser desenvolvidas em conjunto. Essas

análises foram realizadas com base no conteúdo de 127 vagas para a profissão de *pentester*.

#### 4.1 Frequência de menção das competências

Os resultados da análise de frequência das categorias são apresentados na figura 2, enquanto os números de cada habilidade dentro de sua respectiva categoria são exibidos na figura 3. Nossa apuração revela que a maioria das competências exigidas se enquadram em categorias de conhecimento técnico e estão relacionadas à programação, redes de computadores e segurança digital. As principais classes de habilidades são: segurança de redes e sistemas computacionais (23,63%), certificações (15,23%), envolvimento com a comunidade (10,48%), linguagens de programação (10,09%) e redes de computadores (9,70%). Por outro lado, foram identificadas poucas referências a aptidões relacionadas a habilidades sociais, sendo a principal delas a habilidade de comunicação (5,47%), capitaneada essencialmente pela exigência de domínio de línguas estrangeiras.

Figura 2 – Categorias de requisitos demandados em anúncios de vaga para *pentester* no estudo (%).

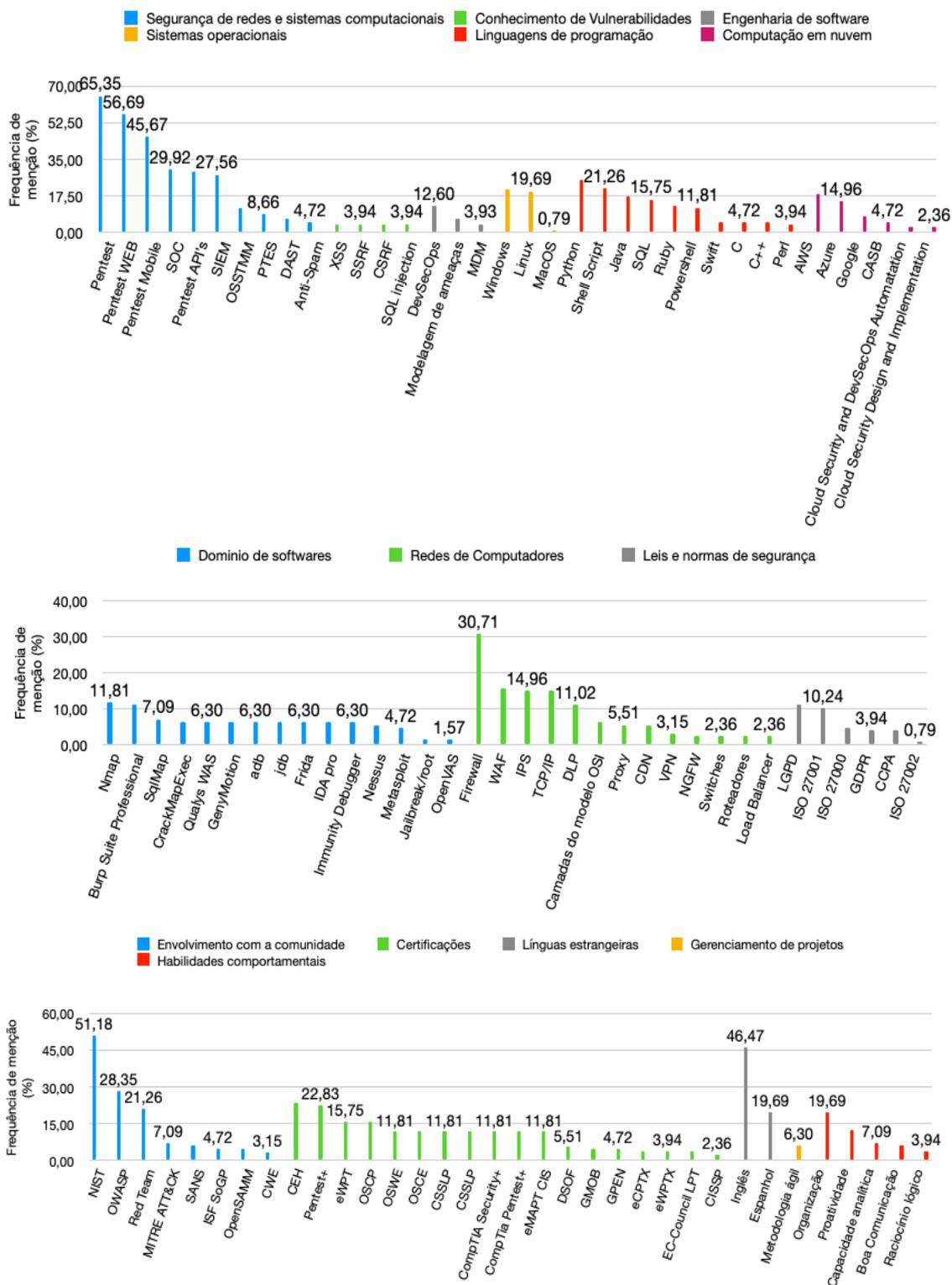


A análise da frequência de menção das competências revela um primeiro panorama indicativo de quais são mais relevantes para *pentesters* no Brasil. Como era de se esperar, a habilidade fundamental é a realização de testes de penetração (*Pentest*) (65,35%), que envolve a avaliação da segurança de sistemas e redes por meio da simulação de ataques de fontes maliciosas. Compreender os testes de penetração específicos para *web* (*Pentest WEB*) (56,69%) e ter conhecimento dos padrões de segurança NIST (51,18%) também são competências extremamente relevantes, pois são mencionadas em mais da metade das vagas. O *National Institute of Standards and Technology* (NIST) estabelece diretrizes para mitigar os riscos cibernéticos organizacionais com base em padrões e boas práticas existentes.

Habilidades em inglês (46,47%), testes de penetração em dispositivos móveis (*Pentest Mobile*) (45,67%), Firewall (30,71%), SOC (Security Operations Center) (29,92%), testes de penetração em APIs (*Pentest API's*) (29,13%), OWASP (Open Web Application Security Project) (28,35%), SIEM (Security Information and Event Management) (27,56%) e Python (25,20%) são menos comuns, mas ainda podem ser consideradas competências-chave. Firewall é um sistema de segurança, tipicamente de rede, que bloqueia ou permite seletivamente pacotes de dados. Já SOC denota uma equipe de profissionais de segurança de TI que monitora a infraestrutura computacional de uma organização a fim de detectar eventos de segurança cibernética em tempo real e solucioná-

los de forma eficaz. OWASP é uma fundação sem fins lucrativos que fornece recursos, ferramentas, diretrizes e conhecimentos para ajudar organizações a desenvolver, adquirir e manter aplicativos *web* seguros.

Figura 3 – Frequência da menção de competências em anúncios de vaga para pentester no Brasil.



Por fim, o SIEM é uma solução de *software* que permite a coleta, correlação e análise de eventos de segurança em tempo real. Outras competências variam de acordo com as tarefas específicas exigidas pelos *pentesters* em diferentes empresas, como conhecimento de linguagens de programação, participação em comunidades, domínio de softwares ou sistemas operacionais específicos. Nesse esse último aspecto, destacam-se os sistemas Windows (20,47%) e Linux (19,69%), com uma baixa frequência de menção ao ambiente MacOS (0,79%).

As habilidades sociais são menos comumente exigidas no trabalho de Pentest no Brasil em comparação com as habilidades técnicas. Por exemplo, a categoria de línguas estrangeiras é a mais importante nesse aspecto, uma vez que o inglês é requisitado em quase metade das vagas e o espanhol em aproximadamente 1 a cada 5 vagas. Além disso, habilidades comportamentais relacionadas à boa organização também são relevantes. No entanto, habilidades de comunicação eficaz, proatividade, capacidade analítica e raciocínio lógico não são frequentemente mencionadas nos requisitos de trabalho de um *pentester*. Em resumo, os requisitos para um *pentest* estão concentrados principalmente nas habilidades técnicas. Isso significa que o profissional deve ser capaz de programar, realizar testes de penetração, estar familiarizado com as boas práticas da área, conhecer vulnerabilidades, ter envolvimento com a comunidade e estar atualizado sobre as leis relacionadas ao assunto. Esses resultados são compreensíveis e esperados, dado que as atribuições e atividades de um *pentester* são extremamente técnicas. Portanto, é natural que as habilidades sociais sejam menos valorizadas nesse contexto.

Uma constatação que pode ser considerada surpreendente é a baixa ocorrência (3,94%) de referências a tipos populares de vulnerabilidades, como XSS, SSRF, CSRF e SQL *injection*. Tendo em vista a elevada frequência de menções a Pentest Web, era de se esperar que esse tipo de conhecimento também fosse exigido em grande parte das ofertas de vagas para *pentesters*. Essa discrepância pode estar relacionada ao fato de que, em muitas organizações, o setor de recursos humanos redige a descrição das vagas sem o auxílio de especialistas da área de *pentest*, ou com uma supervisão superficial e pouco criteriosa. Outra possibilidade é que a maioria das vagas sejam destinadas a profissionais que estão ingressando na carreira. Nesse caso, pode ser exagerado exigir conhecimentos técnicos mais profundos.

#### 4.2 Influência e correlação entre as competências

AA Figura 4 apresenta a rede de interações entre os diferentes requisitos profissionais construída no programa Gephi. As cores e os tamanhos dos nós e textos indicam a influência de cada competência na rede. Quanto mais verde, maior é a influência da competência, enquanto mais rosa indica menor influência. O tamanho do nó e do texto também refletem a importância da competência. Além disso, as linhas entre os nós representam as conexões entre eles. Essa análise considerou o peso das relações entre os nós, sendo que linhas mais grossas indicam maior peso e, conseqüentemente, uma conexão mais forte entre as competências. Uma versão em alta resolução dessa rede está disponível no repositório do projeto no GitHub (PENTESTER, 2013).

Entre as competências que mais se destacam segundo a rede de interações estão: Pentest, Pentest WEB, Pentest Mobile e Pentest API. É um resultado esperado, considerando-se que *pentest* é uma expressão central, pois representa o nome mais usado para expressar a atividade desempenhada pelos profissionais que executam testes de invasão. Porém, é possível depreender também desse resultado que a indústria de



organizações têm papel fundamental em projetos extremamente populares, como o OWASP Top 10, que visam padronizar e orientar procedimentos de segurança.

A fluência em língua inglesa é mais uma competência que aparece em destaque na rede de interações. Essa importância também parece coerente, pois a esmagadora maioria das publicações técnicas sobre cibersegurança são divulgadas em inglês. Apesar de receber menor destaque, a língua espanhola também merece menção.

Entre as certificações também não há surpresas em relação ao resultado aferido com a frequência de menção das competências. CEH e Pentest+ são consideradas mais relevantes, seguidas de eWPT e OSCP. É difícil levantar causas para a maior popularidade das duas primeiras, mas talvez isso esteja relacionado ao fato de que elas são exames de caráter teórico, enquanto eWPT e OSCP são provas práticas.

Conforme ilustrado na Figura 3, outras 7 certificações apresentaram uma frequência de menção muito próxima de eWPT e OSCP. No entanto, a rede de interações não as posicionou entre as competências mais relevantes. Esse fato indica que eWPT e OSCP são mais frequentemente mencionadas junto com outras habilidades mais relevantes para um pentester do que as outras 7 certificações. De maneira similar, Firewall e SIEM são soluções com considerável frequência de citações nos anúncios catalogados (próximo de 30%). São tão mencionadas quanto SOC e PentestAPI, por exemplo. Porém, sua representatividade é pequena na ótica da rede de interações. Essa observação sugere que embora sejam mencionadas em muitas vagas, as competências Firewall e SIEM não parecem muito relacionadas com outras habilidades que têm grande peso na rede de interações.

De maneira mais geral, é possível estabelecer algumas possíveis causas para disparidades de resultados entre a frequência de menções e a representatividade de competências estabelecida através da rede de interações, entre elas:

- Relações espúrias. Pode haver casos em que certas palavras ocorrem juntas em vagas de emprego por razões casuais ou específicas de um determinado conjunto de vagas. Essas relações espúrias podem distorcer o resultado da rede de interações;
- Contexto específico das vagas. As palavras mais frequentes podem estar relacionadas a requisitos básicos e comuns a todas as vagas de *pentesters*, como conhecimentos fundamentais e habilidades técnicas essenciais. Porém, a rede de interações leva em consideração a relevância das palavras com base em suas relações com outras palavras específicas encontradas nas vagas. Portanto, algumas palavras menos frequentes podem ter relações mais significativas com termos específicos do campo de atuação, o que as torna mais relevantes nesse contexto. Esse parece ser o caso das expressões "Red Team" e "SOC";
- Diversidade de vagas. A rede de interações considera a importância das palavras com base na sua ocorrência em diferentes contextos. Se as palavras menos frequentes aparecerem em um conjunto diversificado de vagas, mas com relações mais significativas entre elas, elas podem ser consideradas mais relevantes em comparação com palavras altamente frequentes, mas com relações menos representativas. Considerando que as palavras nmap e SQL não constam entre as expressões mais mencionadas, possivelmente elas aparecem em destaque no resultado da rede de interações por esse motivo;

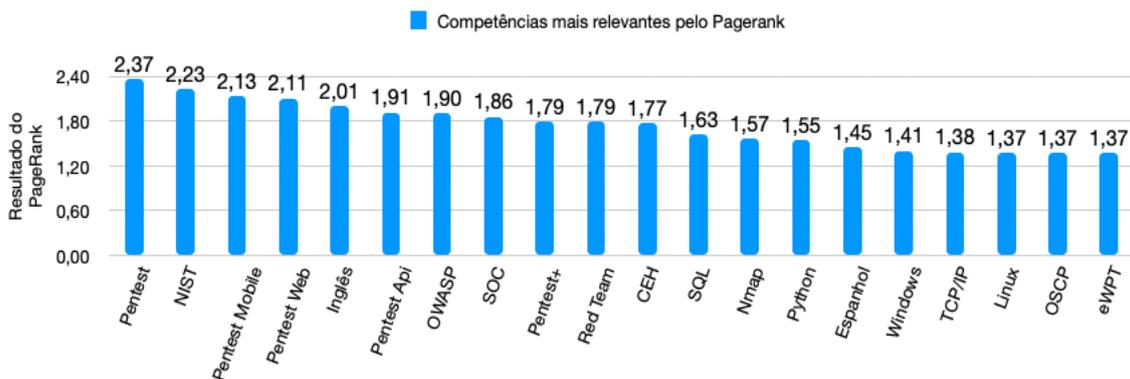
- Variação nas descrições das vagas. Pode haver variações na maneira como as competências são descritas nas vagas de emprego. Algumas palavras podem ser substituídas por sinônimos ou termos relacionados, o que pode levar a uma menor frequência de ocorrência, apesar da importância dessas expressões.

Apesar dessas variações, de modo geral, o resultado ilustrado na figura 4 reforça a confiabilidade da análise da frequência de menção, uma vez que as competências mais citadas também são as mais influentes na rede. É interessante analisar também quais pares de competências devem ser aprendidos em conjunto. Por exemplo, duas competências que foram pouco citadas, mas estão relacionadas, são MacOs e Jailbreak/root. Isso faz sentido, uma vez que o Jailbreak é um processo que permite que dispositivos com sistema iOS executem aplicativos não autorizados pela fabricante Apple. É provável que um empregador que busca um profissional com conhecimentos em MacOs também esteja interessado em realizar Jailbreak em dispositivos iOS. Outros requisitos mencionados em conjunto, apesar de não parecerem ter uma ligação direta à primeira vista, são: Cloud Security and DevSecOps Automation (Segurança na nuvem e automação DevSecOps), Cloud Security Design and Implementation (Projeto e implementação de segurança na nuvem) e CISSP (Certified Information System Security Professional). Embora a certificação CISSP possa não parecer diretamente relacionada às demais competências de computação em nuvem, uma análise mais aprofundada revela que um dos requisitos dessa certificação é a segurança em telecomunicações, redes e internet. Isso pode explicar por que essas competências são solicitadas em conjunto. Esse tipo de rede de interações pode ser utilizado para outras análises específicas, a critério do pesquisador, como identificar as competências mais exigidas em conjunto com uma linguagem de programação específica.

### 4.3 Algoritmo PageRank

A figura 5 apresenta as 20 principais competências classificadas pelo algoritmo PageRank.

Figura 5 – Competências mais relevantes pelo PageRank.



Segundo o algoritmo PageRank, as competências na área de segurança de redes e sistemas computacionais são fundamentais, incluindo habilidades em testes de penetração e compreensão de SOC. Em relação às linguagens de programação, Python e SQL são as mais importantes a serem aprendidas. No que diz respeito ao envolvimento com a comunidade, é interessante conhecer NIST, OWASP e Red Team. O domínio do inglês é a habilidade linguística mais relevante, seguida pelo espanhol. Também é benéfico buscar certificações como Pentest+, CEH (Certified Ethical Hacker), OSCP (Offensive Security

Certified Professional) e eWPT (eLearnSecurity Web Application Penetration Tester). O software mais importante a ser dominado é o Nmap. É essencial ter conhecimento tanto em sistemas operacionais Windows quanto Linux.

Os resultados do algoritmo PageRank são bastante similares àqueles obtidos com as outras técnicas, especialmente a rede de interações entre as competências. A diferença mais marcante é a mesma apontada pela rede de interações: enquanto Firewall (6º) e SIEM (10º) figuram entre as 10 competências mais importantes segundo a frequência de menções, essas habilidades sequer aparecem na lista dos 20 requisitos mais importantes de acordo com a classificação realizada pelo PageRank. Por outro lado, as 5 competências consideradas mais relevantes são as mesmas, com uma ligeira alteração na ordem entre elas. Merece destaque também a ascensão, segundo o PageRank, das competências Pentest Mobile e Pentest API. Esse resultado vai de encontro ao relatório divulgado por uma pesquisa recente que destaca o crescimento de aplicações Web e APIs como superfícies de ameaças em 2022 (AKAMAI, 2023).

## 5. Conclusão

Neste estudo, identificamos a estrutura de competências necessárias para profissionais de pentesting no Brasil. Utilizando técnicas de web scraping, coletamos informações de 207 vagas de emprego, das quais 127 foram consideradas relevantes. Por meio da análise da frequência de menção, influência e correlação, bem como do algoritmo PageRank, obtivemos revelações valiosas sobre as habilidades mais demandadas e sua interconexão. Os resultados revelaram que, no Brasil, os empregadores buscam pentesters com conhecimentos técnicos nas áreas de redes, aplicações móveis ou sistemas web, preferencialmente certificados. A fluência em inglês também é considerada um fator preponderante.

Esses resultados têm implicações significativas para o desenvolvimento de currículos e programas educacionais em segurança digital. Eles fornecem orientações para que as instituições educacionais possam ajustar o conteúdo das disciplinas, permitindo que os alunos e profissionais adquiram um perfil de competências mais alinhado às demandas do mercado de trabalho. Além disso, responsáveis por contratações de pentesters podem se beneficiar dessas descobertas ao compreenderem melhor as competências essenciais e definirem requisitos de trabalho mais precisos, resultando em economia de recursos e de tempo. É importante destacar que este estudo focou em vagas de emprego no Brasil. Estudos futuros podem considerar a pesquisa em outros países, proporcionando uma compreensão mais abrangente das tendências globais nessa área.

## Referências

AKAMAI. <https://www.akamai.com/pt/resources/state-of-the-internet/slipping-through-the-security-gaps-the-rise-of-application-and-api-attacks>. Relatório SOTI de apps e APIs. 2023.

ANTHONY JNR, B. Managing digital transformation of smart cities through enterprise architecture-a review and research agenda. **Enterprise Information Systems**. V15. N.3 p. 299-331. 2021.

BISWAS, R.; BISWAS, R. Disruptive change from robotics, industrial automation and the digital economy. **Emerging markets megatrends**. p. 135-147. 2018.

- BRIN, S.; PAGE, L. Reprint of: The anatomy of a large-scale hypertextual web search engine. **Computer networks**. V56. N.18 p. 3825-3833. 2012.
- CALANCA, F.; SAYFULLINA, L.; MINKUS, L.; WAGNER, C.; MALMI, E. Responsible team players wanted: an analysis of soft skill requirements in job advertisements. **EPJ Data Science**. V8. N.1 p. 1-20. 2019.
- CETIC.BR. <https://cetic.br/pt/publicacao/resumo-executivo-pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2020> Pesquisa TIC domicílios. 2020.
- CHERVEN, K. **Network graph analysis and visualization with Gephi**. 2013.
- DE SILVA, R.; RUPASINGHE, T. D.; APEAGYEI, P. A collaborative apparel new product development process model using virtual reality and augmented reality technologies as enablers. **International Journal of Fashion Design, Technology and Education**. V12. N.1 p. 1-11. 2019.
- DUTRA, T. N. A.; CARVALHO, A. V. O profissional da informação e as habilidades exigidas pelo mercado de trabalho emergente. **Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação**. V11. N.22 p. 178-194. 2006.
- EDUARDO, M.; AFANASEV, V.; ZHUSTEC. <https://github.com/vifreefly/kimuraframework> **Kimurai**. 2023.
- ESTADÃO. <https://www.estadao.com.br/economia/negocios/ciberseguranca-salario-cursos-ti/>. Demanda por cibersegurança faz salário disparar e multiplica cursos de TI. 2022.
- FUNDAÇÃO GETÚLIO VARGAS. <https://portal.fgv.br/noticias/pandemia-acelerou-processo-transformacao-digital-empresas-brasil-revela-pesquisa>. Pandemia acelerou processo de transformação digital das empresas no Brasil. 2022.
- GABOR, D.; BROOKS, S. The digital revolution in financial inclusion: international development in the fintech era. **New political economy**. V22. N.4 p. 423-436. 2017.
- GARDINER, A.; AASHEIM, C.; RUTNER, P.; WILLIAMS, S. Skill requirements in big data: A content analysis of job advertisements. **Journal of Computer Information Systems**. V58. N.4 p. 374-384. 2018.
- GIORDANO, A.; PAGANO, A. The Chinese policy of highly-qualified human capital: a strategic factor for global competition in innovation. **Transition Studies Review**. V19. p. 325-337. 2013.
- GOLDSMITH, A.; SALEHUDDIN MOHD ZAHARI, M. Hospitality education in Malaysia: Filling the skill gap. **International Journal of Contemporary Hospitality Management**. V6. N.6 p. 27-31. 1994.
- HOSU, I.; IANCU, I. Digital entrepreneurship and global innovation. **IGI Global**. 2016.
- ISC2. <https://www.isc2.org/-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx>. **Cybersecurity Workforce Study**. 2022.
- TOBIAS, L. <https://github.com/leonardobotrel/Perfil-pentester>. Identificação do perfil de pentester desejado pelas empresas brasileiras. 2023.

TAMER, C.; VIANA, C.; SOARES, L. A.; LIMA, M. Perfil do profissional contábil demandado pelo mercado de trabalho: um estudo no norte do Brasil. **Revista Universo Contábil**. V9. N.3 p. 143-162. 2013.

TONELLI, A. C. d. S. <https://repositorio.ufsc.br/handle/123456789/197895>. **O perfil atual do profissional de controladoria requerido pelas empresas brasileiras**. 2019.

WORTMANN, F.; FLÜCHTER, K. Internet of things: technology and value added. **Business & Information Systems Engineering**. V57. p. 221-224. 2015.