

# Protocolo de busca a Testes de Penetração em dispositivos móveis

**Guilherme Leal Kaiser, Daniel Dalalana Bertoglio**

Universidade Feevale – Novo Hamburgo – RS – Brasil

guilhermelealkaiser@gmail.com, dalalana@feevale.br

**Abstract.** This article describes the development for a search protocol based on the systematic mapping model, focusing on penetration testing towards mobile devices. It presents data on the importance of the focus to tests in these devices, followed by the systematic mapping model, which through it were developed the planning and conduction stages, ending with the quality analysis of the articles returned from the searches. This protocol is the basis for an upcoming study in order to propose a detailed analysis on the theme, aiming among other reasons to answer the research questions presented here.

**Resumo.** Este artigo descreve o desenvolvimento de um protocolo de busca baseado no modelo de mapeamento sistemático, com foco em testes de penetração voltado a dispositivos móveis. Ele apresenta dados da importância do foco a testes nesses dispositivos, seguido do modelo de mapeamento sistemático. Através dele foram desenvolvidas as etapas de planejamento e condução, finalizando com a análise de qualidade dos artigos retornados das buscas. Esse protocolo, por fim, é a base para um próximo estudo a fim de propor uma análise detalhada sobre o tema, visando, dentre outras razões, responder as questões de pesquisa aqui apresentadas.

## 1. Introdução

Atualmente, a segurança de informações tem representado com notoriedade parte das pesquisas relacionadas ao tratamento, prevenção e proteção de dados, processos e tecnologias. Em paralelo a isso, com o crescente uso de dispositivos móveis e o consequente aumento no tráfego de dados gerados pelos mesmos, as preocupações com riscos e vulnerabilidades ampliaram a atuação dessas pesquisas para contribuições voltadas a teste e avaliação de segurança. Uma das técnicas de teste de segurança é o teste de penetração, mais conhecido como *Pentest*. *Pentest*, segundo Bertoglio (2017), é o nome dado à tentativa controlada de penetrar um sistema ou rede a fim de detectar vulnerabilidades.

Segundo o terceiro relatório anual emitido pela Juniper Networks Inc (2013), a crescente dependência de dispositivos inteligentes provou ser um alvo irresistível para os invasores, pois eles estão rapidamente eclipsando computadores na era pós-PC. Nesse sentido, é igualmente relevante indicar a grande proliferação de softwares maliciosos nas diversas plataformas móveis, em particular na plataforma Android, a qual não obteve uma resposta rápida dos fornecedores de produtos de segurança da informação [Braga 2012].

Por esse motivo, foi constatada a importância de gerar uma pesquisa voltada a área, para obter como resultado os últimos estudos e práticas relacionadas.

O estudo, portanto, foi feito de acordo com o modelo de Mapeamento Sistemático proposto por Petersen et al. (2008), que o divide em 3 fases: Planejamento, Condução e Apresentação. No entanto, este protocolo de busca será focado apenas nas etapas de Planejamento e Condução, descritos nas seções quatro e cinco, após as sessões dois e três que trazem uma visão geral sobre *Pentest* e Mapeamento Sistemático, respectivamente. Finalizando, então, com a sessão de lições aprendidas e principais contribuições, seguida da conclusão.

## 2. Pentest

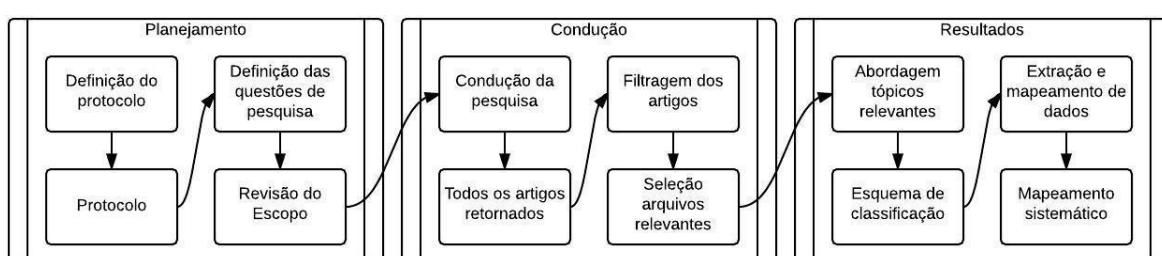
A utilização de *Pentest* visa encontrar vulnerabilidades em um determinado sistema ou rede. Ele também é referido como "*hacking ético*" porque os testadores de penetração investigam o sistema alvo do ponto de vista de um invasor, relatando fraquezas em vez de explorá-las [Bohme 2010]. Há inúmeros benefícios de testes de penetração nos negócios, bem como perspectiva técnica. Algumas das principais razões para a adoção de testes de penetração são: problemas de segurança, priorizar riscos de segurança, perda financeira [Stefinko 2016].

Um *Pentest* pode ser dividido numa série de fases, que quando colocadas juntas formam uma metodologia abrangente para completar um teste de penetração [Ramos 2013]. Dentre elas tem-se o escopo de metas, o recolhimento de informações, a descoberta de destino, a enumeração do alvo, o mapeamento de vulnerabilidades, a engenharia social, a exploração de destino, a escalação de privilégios, a manutenção do acesso e a documentação e relatórios [Stefinko 2016].

## 3. Mapeamento Sistemático

O protocolo de busca foi baseado no modelo de mapeamento sistemático que, segundo Santos (2015), é uma forma de identificar, avaliar e interpretar todas as pesquisas disponíveis relevantes para uma questão de pesquisa particular. Conforme Petersen et al. (2008), dentre as etapas essenciais do processo estão a definição de questões de pesquisa, a realização de pesquisas relevantes, triagem de documentos, palavras-chave de abstrações e extração e mapeamento de dados.

Todas as etapas do mapeamento sistemático estão apresentadas na Figura 1, que traz o fluxo em que elas ocorrem durante o mapeamento.



**Figura 1. Processo de estudo de mapeamento sistemático.**

Este artigo, conforme mencionado anteriormente, trará apenas o protocolo final da busca para um futuro mapeamento sistemático, que englobará as partes de planejamento e condução, descritas na sequência.

#### **4. Planejamento**

Esta pesquisa tem como foco planejar e executar uma busca nos moldes de um mapeamento sistemático com base no tema de testes de penetração em dispositivos móveis.

A estrutura da questão desta pesquisa foi baseada segundo a proposta trazida por Kitchenham [2007 apud Bertoglio 2017] que a organiza nos critérios de PICO (*Population, Intervention, Comparison, Outcome*):

- População (*Population*): artigos de pesquisa relacionados à área de Segurança da Informação.
- Intervenção (*Intervention*): testes de penetração.
- Controle (*Comparison*): dispositivos móveis.
- Resultados (*Outcome*): obter uma análise sobre testes de penetração em dispositivos móveis para identificar as ferramentas, metodologias de testes e possíveis falhas de segurança encontradas nos modelos analisados.

Foram descritas cinco questões de pesquisa (Q) e estas são apresentadas na sequência.

**Q1.** Quais são as principais ferramentas utilizadas neste modelo de *Pentest*?

**Q2.** Quais as principais falhas identificadas?

**Q3.** Quais os dispositivos móveis mais utilizados nos testes?

**Q4.** Quais os cenários de execução dos *Pentests* em dispositivos móveis?

**Q5.** Quais as principais limitações/desafios?

Com relação ao processo de pesquisa, foram selecionadas bases de dados que contém modelo de busca baseado em palavras chave em artigos da área da ciência da computação, escritos em português ou inglês. Dentre as selecionadas estão ACM Digital Library, IEEE Xplore, Scopus e Springer Link.

Já os termos e sinônimos usados na *string* de busca foram divididos também com base nos critérios de PICO, mostrados anteriormente. A **Tabela 1** apresenta essas divisões.

**Tabela 1. Termos e sinônimos organizados de acordo com a estrutura (critérios de PICO)**

ESTRUTURA	TERMOS	SINÔNIMOS
<i>População</i>	<i>Security Information</i>	
<i>Intervenção</i>	<i>Penetration Test</i>	<i>Security Test, Security Testing, Penetration Testing, Pentest</i>
<i>Controle</i>	<i>Mobile Devices</i>	<i>Mobile</i>
<i>Resultados</i>	<i>Tool</i>	<i>Tools, Software, Program, Application</i>
	<i>Vulnerability</i>	<i>Flaw</i>

	<i>Mobile Operation System</i>	<i>Android, Ios</i>
	<i>Model</i>	<i>Process, Method, Framework, Methodology</i>
	<i>Scenarios</i>	<i>Context, Environment</i>
	<i>Challenges</i>	<i>Open Problems, Open research topics</i>

Nas *strings* de busca foi utilizado o operador “OR” para selecionar os termos e sinônimos, e o operador “AND” para selecionar os termos da estrutura da questão: população, intervenção, controle e resultados. Devido ao retorno negativo de artigos com a *string* completa nas bases Scopus, IEEE e ACM, foi necessário realizar as buscas com *strings* reduzidas conforme apresentado na Figura 2:

<b>Scopus:</b>
(“Security Test” OR “Security Testing” OR “Penetration Test” OR “Penetration Testing” OR “Pentest”) AND (“Mobile Devices” OR “Mobile”) AND (“Tool” OR “Tools” OR “Software” OR “Program” OR “Application”) AND (“Vulnerability” OR “Flaw”)
<b>IEEE e ACM:</b>
(“Security Test” OR “Security Testing” OR “Penetration Test” OR “Penetration Testing” OR “Pentest”) AND (“Mobile Devices” OR “Mobile”)

**Figura 2. *Strings* reduzidas utilizadas para a busca nas bases de dados especificadas.**

Foram descritos dois critérios de inclusão (IC) e dois de exclusão (EC), que são de grande importância para a apuração dos resultados. Tais critérios são responsáveis por apoiar a seleção dos artigos apropriados e são empregados para reduzir o número de artigos que retornam das *engines* de busca [Bertoglio 2017].

- IC1.** O tema principal traz um estudo sobre *Pentests* em dispositivos móveis;
- IC2.** O estudo principal propõe um modo para prover *Pentests* em dispositivos móveis;

- EC1.** O estudo principal não está relacionado diretamente a *Pentests* em dispositivos móveis;

- EC2.** O estudo principal não contém algum tipo de avaliação para demonstrar os resultados;

Na parte de avaliação de qualidade (*Quality Assessment - QA*), que visa mensurar a relevância de cada um dos estudos retornados, foram definidos três critérios, identificados com as questões:

- QA1.** O estudo apresenta uma contribuição ao tema de *Pentest* em dispositivos móveis?

- QA2.** O estudo descreve as ferramentas ou modelos utilizados?

- QA3.** Apresenta uma avaliação das ferramentas e/ou modelos utilizados em *Pentests* direcionados a dispositivos móveis?

Para cada uma das questões dos critérios de qualidade é utilizada a seguinte pontuação: Y (sim) = 1; P (parcialmente) = 0,5, N (não) = 0. Com isso, o *Score* (soma das três questões) pode classificar os estudos em: 0 ou 0,5 (limitado), 1 (regular), 1,5 (bom), 2 (muito bom) e 2,5 ou 3 (excelente).

O processo de seleção foi dividido em quatro etapas: busca nas bases de dados, eliminação das redundâncias, seleção final e avaliação da qualidade. Estas são descritas na sequência.

- Busca nas bases de dados: nesta etapa foram utilizadas as *strings* de busca geradas a partir dos termos e sinônimos, para fazer a procura nas bases de dados selecionadas.
- Eliminação das redundâncias: após a busca foram eliminadas e armazenadas as redundâncias.
- Seleção final: nesta etapa o título e o resumo de cada artigo retornado das buscas são lidos, e com base nos critérios de inclusão e exclusão é feita a seleção dos que serão utilizados.
- Avaliação da qualidade: concluída a etapa de seleção final, os artigos selecionados são lidos e analisados de acordo com os critérios de qualidade.

## 5. Condução

A condução deste protocolo detalha os resultados obtidos após as etapas do processo de seleção. Tendo como resultado um total de 286 artigos após a primeira leitura, 41 foram eliminados e arquivados na fase de eliminação de redundâncias. Já na terceira, que representa a seleção final, atingiu-se como resultado 33 artigos. Na etapa final do processo de seleção, os 33 artigos selecionados foram avaliados com base nos critérios de qualidade mostrados anteriormente. Segundo Bertoglio (2017), tais critérios ajudam a avaliar a confiabilidade dos estudos. A **Tabela 3** traz o resultado dessa avaliação feita por artigo, detalhando o ano e a referência de cada um deles. Ela exibe nas colunas 1, 2, 3 os *scores* relacionadas a *Quality Assessment* (QA) e na coluna *Sc* traz o *score* final, classificando cada artigo de acordo o Sc obtido, conforme mostra a coluna Des.

**Tabela 3. Resultados da análise da qualidade por artigo**

<b>Estudos</b>		<b>QA</b>		<b>Qualidade</b>		<b>Estudos</b>		<b>QA</b>		<b>Qualidade</b>					
ID	Referência	Ano	1	2	3	Sc	Des	ID	Referência	Ano	1	2	3	Sc	Des
1	Morais	2011	P	Y	Y	2,5	E	18	Sadeghi	2014	P	P	N	1	R
2	Habib	2008	P	Y	P	2	M	19	Jadhav	2015	Y	P	P	2	M
3	Mahmood	2012	Y	Y	Y	3	E	20	Wang	2015	Y	Y	P	2,5	E
4	Habib	2009	Y	Y	Y	3	E	21	Lee	2015	Y	Y	Y	3	E
5	Wang	2015	P	Y	N	1,5	B	22	Knorr	2015	P	P	Y	2	M
6	Wu	2014	Y	Y	Y	3	E	23	Koivunen*	2016				0	L
7	Wu	2015	P	Y	N	1,5	B	24	Yang	2016	Y	Y	Y	3	E
8	Gagnon	2016	Y	Y	Y	3	E	25	Debbabi	2005	Y	Y	Y	3	E
9	Salva	2015	P	Y	Y	2,5	E	26	Knorr	2015	Y	Y	Y	3	E
10	Brandt	2014	Y	Y	Y	3	E	27	Hunt	2013	Y	Y	Y	3	E

11	Salva	2013	P	P	P	1,5	B	28	Avancini	2013	Y	P	P	2	M
12	Fahrianto	2016	Y	P	P	2	M	29	Bojjagani*	2016				0	L
13	Debbabi*	2006				0	L	30	Badura	2009	P	P	P	1,5	B
14	Abgrall	2014	P	P	Y	2	M	31	Javed	2014	Y	Y	Y	3	E
15	Morais	2012	P	Y	Y	2,5	E	32	Mulliner	2009	Y	Y	Y	3	E
16	Noponen	2008	Y	Y	P	2,5	E	33	Mulliner	2006	Y	P	P	2	M
17	Salva*	2013				0	L								

**Legenda:** Y: Sim, N: Não, P: Parcialmente, Sc: Score, Des: Descrição, B: Bom, M: Muito Bom, E: Excelente, R: Regular, L: Limitado

\*Artigos que não se obteve acesso para avaliação da qualidade.

## 6. Lições Aprendidas e Principais Contribuições

Após a análise de qualidade concluída, obteve-se um protocolo de busca base para realização de um mapeamento sistemático, que pode, além disso, ser uma fonte de pesquisa focada ao assunto, provendo estudos que foram classificados de acordo com a sua relevância ao mesmo. Além disso na análise de qualidade foram considerados como que respondendo parcialmente a primeira questão, estudos que demonstram ou provem maneiras de examinar os dispositivos ou aplicativos a fim de identificar possíveis vulnerabilidades. Tais estudos não foram desconsiderados por seu assunto não ser diretamente relacionado a *Pentest* porque as análises trazidas por eles poderão ser usadas na fase de mapeamento de vulnerabilidades dos testes.

Por fim, como principal contribuição e motivação está à busca em estabelecer aos interessados no assunto uma amostra de como estão os principais estudos, junto com a sua análise inicial já concluída. Indicando, além disso, os autores que desempenharam algum esforço nesta área, para se necessário poder ser feita uma busca específica a outros trabalhos realizados por eles.

## 7. Conclusão

Como citado anteriormente, a área relacionada a testes de segurança tem crescido nos últimos tempos, tendo como grande fator a busca pela segurança da informação. E *Pentests* aparecem como um dos principais, pois visam verificar vulnerabilidades para, a partir delas, analisar seu risco e impacto ao sistema direcionado, a fim de prevenir possíveis ataques.

Foi visando o crescente estudo nesta área que o protocolo de busca teve como foco preparar a pesquisa para um futuro mapeamento sistemático a testes de penetração em dispositivos móveis, já que esses dispositivos estão a cada dia mais presentes, armazenando, realizando tarefas e transações com dados de valor significativo para os usuários.

A partir deste tema o protocolo de busca obteve o conteúdo primário para o estudo nesta área, após toda a busca, seleção e análise da qualidade dos artigos relevantes. Na última etapa pode-se chegar a uma qualidade significativa, já que 72% dos estudos obtiveram score final entre 2 e 3 pontos, classificando-os, assim, como muito bons ou excelentes. Outro ponto importante a ser analisado é que também 72% dos estudos finais que tiveram a sua

qualidade avaliada foram realizados nos últimos cinco anos, ou seja, são estudos recentes na área.

Com isso foi possível perceber o quanto importante é o enfoque deste protocolo, reunindo informações sobre um estudo relevante para o contexto atual, mas que tem suas pesquisas e testes muito recentes ainda. E é isso o que motiva o próximo trabalho, que a partir do conteúdo aqui obtido irá propor uma análise detalhada sobre este enfoque e modelo de teste de segurança, visando, dentre outras razões, responder as cinco questões de pesquisa apresentadas neste protocolo.

## Referências

- Petersen K, Feldt R, Mujtaba S, Mattsson M. (2008). “Systematic mapping studies in software engineering”. In: Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering. EASE’08. British Computer Society, Swinton. pp 68–77.
- Bertoglio D. Dalalana, Zorzo A. Francisco (2017). “Overview and open issues on Penetration test”.
- Juniper networks - Mobile Threat Center Third Annual Mobile Threats Report: March 2012 through March 2013.
- Habib S. Mahbub, Jacob Cyril, Olovsson Tomas (2008). “A Practical Analysis of the Robustness and Stability of the Network Stack in Smartphones”. In: Department of Computer Science & Engineering, Chalmers University of Technology, Gothenburg, SE-41296, Sweden.
- Mahmood Riyadh, Esfahani Naeem, Kacem Thabet, Mirzaei Nariman, et al. (2012). “A Whitebox Approach for Automated Security Testing of Android Applications on the Cloud”. Disponível em: Computer Science Department George Mason University.
- Bohme Rainer, Felegyhazi Mark (2010). “Optimal Information Security Investment with Penetration Testing”. In: International Computer Science Institute, Berkeley, California
- Stefinko Yaroslav, Piskozub Andrian, Banakh Roman (2016). “Manual and Automated penetration testing. Benefits and Drawbacks. Modern tendency”.
- Braga A. Melo, Nascimento E. Nogueira, Palma L. Rodrigues, Rosa R. Pereira (2012). “Introdução à Segurança de Dispositivos Móveis Modernos – Um Estudo de Caso em Android”.
- Ramos J. J. Afonso (2013). “Sistema Automático para Realização de Testes de Penetração”
- Morais Anderson, Cavalli Ana, Martins Eliane (2011). “A model-based attack injection approach for security validation”.
- Habib Sheikh Mahbub, Jacob Cyril, Olovsson Tomas (2009). “An Analysis of the Robustness and Stability of the Network Stack in Symbian-based Smartphones”.
- Wang Yong (2015). “An Automated Virtual Security Testing Platform for Android Mobile Apps”.

- Wu Daoyuan, Chang Rocky K. C. (2014). “Analyzing Android Browser Apps for file:// Vulnerabilities”.
- Wu Jingzheng, Wu Yanjun, Wu Zhifei, Yang Mutian, et. al (2015). “AndroidFuzzer: Detecting android vulnerabilities in fuzzing cloud”.
- Gagnon François, Ferland Marc-Antoine, Fortier Marc-Antoine, Desloges Simon, et. al (2016). “AndroSSL: A Platform to Test Android Applications Connection Security”.
- Salva Sébastien, Zafimiharisoa Stassia R. (2015). “APSET, an Android aPplication SEcurity Testing tool for detecting intent-based vulnerabilities”.
- Brandt N. Benecke, Stamp Mark (2014). “Automating NFC message sending for good and evil”.
- Salva Sébastien, Zafimiharisoa Stassia R. (2013). “Data vulnerability detection by security testing for Android applications”.
- Fahrianto Feri, Lubis M. Fadil, Fiade Andrew (2016). “Denial-of-Service attack Possibilities on NFC Technology”.
- Abgrall Erwan, Traon Y. Le, Gombault Sylvain, Monperrus Martin (2014). “Empirical Investigation of the Web Browser Attack Surface under Cross-Site Scripting: An Urgent Need for Systematic Security Regression Testing”.
- Morais Anderson, Hwang Iksoon, Cavalli Ana, Martins Eliane (2012). “Generating attack scenarios for the system security validation”.
- Noponen Sami, Karppinen Kaarina (2008). “Information Security of Remote File Transfers with Mobile Devices”.
- Sadeghi Alireza, Esfahani Naeem, Malek Sam (2014). “Mining the Categorized Software Repositories to Improve the Analysis of Security Vulnerabilities”.
- Jadhav Suyash, Oh Tae, Kim Y. Ho, Kim J. Nyeo (2015). “Mobile device penetration testing framework and platform for the mobile device security course”.
- Wang Yong, Alshboul Yazan (2015). “Mobile Security Testing Approaches and Challenges”.
- Lee W. Hao, Ramanujam M. Srirangam, Krishnan S. P. T. (2015). “On designing an efficient distributed black-box fuzzing system for mobile devices”.
- Knorr Konstantin, Aspinall David, Wolters Maria (2015). “On the Privacy, Security and Safety of Blood Pressure and Diabetes Apps”.
- Yang Yaping, Cai Lizhi, Zhang Yanguo (2016). “Research on non-authorized privilege escalation detection of android applications”.
- Debbabi Mourad, Saleh Mohamed, Talhi Chamseddine, Zhioua Sami (2005). “Security Analysis of Wireless Java”.
- Knorr Konstantin, Aspinall David (2015). “Security Testing for Android mHealth Apps”.
- Hunt Ray (2013). “Security testing in Android networks - A practical case study”.

- Avancini Andrea, Ceccato Mariano (2013). “Security testing of the communication among Android applications”.
- Badura Thomas, Becher Michael (2009). “Testing the Symbian OS Platform Security Architecture”.
- Javed Ashar, Schwenk Jörg (2014). “Towards Elimination of Cross-Site Scripting on Mobile Versions of Web Applications”.
- Mulliner Collin (2009). “Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones”.
- Mulliner Collin, Vigna Giovanni (2006). “Vulnerability Analysis of MMS User Agents”.
- Santos M. Auréli, Barreto R. da Silva (2015). “Mapeamento Sistemático”.
- Salva Sébastien, Zafimiharisoa Stassia R., Laurencot Patrice (2013). “Intent security testing: An Approach to testing the Intent-based vulnerability of Android components”.
- Koivunen Lauri, Rauti Sampsa, Leppänen Ville, et al (2016). “Proceedings - 2016 International Conference on Software Security and Assurance, ICSSA 2016”.
- Debbabi Mourad, Saleh Mohamed, Talhi Chamseddine, Zhioua Sami (2006). “Embedded Java Security: Security for Mobile Devices”.
- Bojjagani Sriramulu (2015). “STAMBA: Security testing for android mobile banking apps”.