Acta Informatica Pragensia, 2016, 5(2): 98–117
DOI: 10.18267/j.aip.88
Peer-reviewed paper

PETA: Methodology of Information Systems Security Penetration Testing

Tomáš Klíma*

Abstract

Current methodologies of information systems penetration testing focuses mainly on a high level and technical description of the testing process. Unfortunately, there is no methodology focused primarily on the management of these tests. It often results in a situation when the tests are badly planned, managed and the vulnerabilities found are unsystematically remediated. The goal of this article is to present new methodology called PETA which is focused mainly on the management of penetration tests. Development of this methodology was based on the comparative analysis of current methodologies. New methodology incorporates current best practices of IT governance and project management represented by COBIT and PRINCE2 principles. Presented methodology has been quantitatively evaluated.

Keywords: IT security, Penetration testing, Methodology, IT security audit.

1 Introduction

In the recent years, we could see many high profile companies such as RSA, Global Payments, Heartland Payment Systems, Sony or LinkedIn to incur a data breach with the significant financial loss (Verizon, 2013; Verizon, 2015; CheckPoint, 2013). In spite of the fact that these organizations had probably all state of the art security controls in place, the intruders were able to breach them and steal the data that were mission critical for some of these companies.

As the current controls seem to be unable to really prevent the security incidents, the IT managers pay more and more attention to the offensive security techniques. These techniques closely mimic the attackers (and emulate the threats) in order to identify as many vulnerabilities of target system as possible. These techniques are known as a security penetration tests and they assess the level of implementation of IT security policy into practice. Exact definition according to the NIST (2008) is "Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network." These tests are usually conducted by an external company, but larger organizations have also in-house teams (red teams) that are responsible for testing the security of IT infrastructure and information systems. In order to understand the role of penetration tests, the reader should be familiar with the model below (Figure 1), which presents a comparison of three basic types of IS security assessment.

* Department of Systems Analysis, Faculty of Informatics and Statistics, University of Economics, Prague, W. Churchill Sq. 4, 130 67 Prague 3, Czech Republic
✉ xklit10@vse.cz

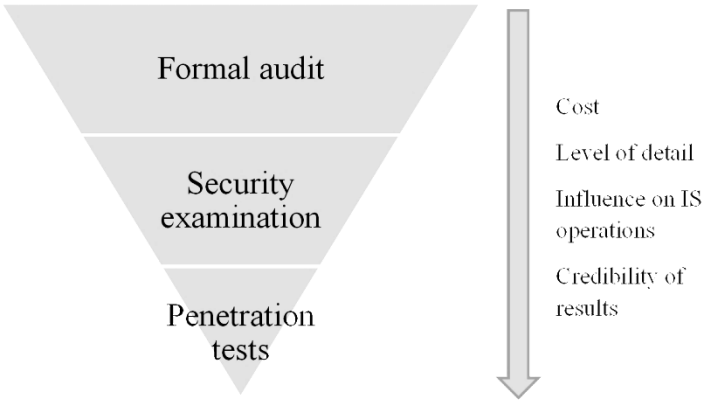

***Fig. 1**. Types of IS security assessment. Source: author.*

The first level of this model is called formal audit. It´s most process-oriented and primarily focuses on policies. Basic methods of the formal audit are interviews with employees and reviews of the documentation and formal description of the processes. The second level is called security examination and focuses mainly on reviews of implementation of security policies, e.g. firewall configuration or network segmentation. Basic methods are security checks or tests. The third level are penetration tests - they are the most technically oriented and deliver the most credible results with the highest level of detail, but are also connected with the highest probability of damaging the target IS and highest costs. In order to conduct a thorough assessment, the organization should employ all three levels. Common practice according to the experience of the author is to combine two levels which are chosen according to the needs of a business owner of target IS. As we can see from the model, penetration tests have the highest level of detail and therefore also potential to identify real vulnerabilities which (if not remediated) could lead to a security incident or a breach, therefore are nowadays considered to be necessary for information systems rated as critical or confidential.

2 Methodology of the research

The goal of this article is to present a design of new methodology, which aims to overcome weaknesses of the current approaches. The new methodology is based on comparative analysis of the current methodologies and has been quantitatively evaluated. The design science research approach was employed as is described in the rest of this section.

The first step was the identification of problems in practical penetration tests. After that, the review of current sources which deal with a penetration testing (and information security in general) was conducted. These sources were further divided into two groups - current methodologies and other sources. Other sources were analyzed in order to select relevant publications which are of interest for deeper understanding of the examined problematics. Comparative analysis of current methodologies was conducted in order to identify their weaknesses and non-covered areas.

As this comparative analysis showed, the main missing area is the management of penetration tests. Therefore the design of new methodology was primarily focused on this topic, which includes integration of penetration tests into the context of IT management and project management of penetration tests (as described in Section 5). The new methodology employs layered and modular approach and is based on current best practices, especially COBIT (ITGI, 2007) and PRINCE2 (Office of Government Commerce, 2009). The significant part of

Section 5 (design of new methodology excluding the topic of integration of penetration test into the context of IT management) has been already presented in (Klima, 2015b).

The methodology has been evaluated on the theoretical and practical level. Description of both types of evaluation is in Section 6. The theoretical evaluation consists of proof that areas missing in current methodologies have been covered. The practical evaluation consists of six penetration tests conducted in the target organization (banking sector, 1000+ employees) managed by PETA (case study). These tests have been quantitatively evaluated (employing a questionnaire where six criteria were evaluated on a scale for each of the tests) by two involved stakeholders (IT security manager and IT operations manager). The results were compared to a control group of two penetration tests managed according to other approaches.

3 Literature review

Most important publications on the problematics are current IS penetration testing methodologies. As they are analyzed in more detail in the next section, we will now focus on other significant works.

At first, there are publications that are important for the definition of basic terminology and for the clarification of the role of the penetration tests in the context of IS/IT (security) management. Most important is Doucek et al. (2011), where the relationship between IS audit, risk analysis and penetration tests is defined. This area is also analyzed in *Audit for Information Systems Security* (Suduc et al., 2010). Other significant publications are *NIST Special Publication 800-53: Security and Privacy Controls for Federal information Systems and Organizations* (NIST, 2013) and *The Critical Security Controls for Effective Cyber Defense* (SANS, 2014), which define the penetration tests as important cyber security measures.

The analysis of the connection between penetration tests and IS/IT (security) management is based on COBIT 4.1 (ITGI, 2007), COBIT 5 (ITGI, 2012) and Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit 2008 (ITGI, 2008). Framework COBIT 4.1 (especially the structure of its processes) is crucial for planning, operational management and implementation of countermeasures. Complementary to the COBIT framework is *IS Auditing procedure: Security assessment - penetration testing and vulnerability analysis* (ISACA, 2004), which is one of the first attempts to use COBIT for the penetration tests. The specific topic of the penetration tests in the banking industry is covered in *Penetration testing in the financial services industry* (SANS, 2010).

The general level of penetration tests is discussed in *Penetration Testing: Assessing Your Overall Security Before Attackers Do* (Northcutt, 2006) and in excellent study *A penetration testing model* (BSI, 2008). Further reading on this topic is *A Conceptual Model Approach to Manage and Audit Information Systems Security* (Pereira & Santos, 2010) and little bit outdated *Improving the Security of Your Site by Breaking Into it* (Farmer & Venema, 1993), which is the pioneer paper on basic penetration methods. Conducting *Penetration Test on an Organization* (Wai, 2002) and *Generally Accepted Principles and Practices for Securing Information Technology Systems: NIST Special Publication 800-14* (Swanson, 1996) are very useful for the understanding of elementary principles of IS security assessment. Classic publication on IS testing is *Test maturity model integration* (TMMi, 2008), which had been employed as an inspiration for creation PETA methodology.

The role of the PCI DSS standard (Payment Card Industry Data Security Standard) as a significant driver of penetration tests is examined in *PCI DSS: Information Supplement:*

Requirement 11.3 Penetration Testing (PCI Security standards council, 2008) and *In-house Penetration Testing for PCI DSS* (Koster, 2012).

Description of the testing process is covered in a great level of detail in *Ethical hacking and countermeasures v7.1* (EC-COUNCIL, 2011) which is a very exhaustive source of information about specific testing techniques and tools. Series of books Hacking exposed cover whole portfolio of topics like web applications (Scambray & McClure, 2008), wireless networks (Cache & Liu, 2007), malware (Davis & Bodmer, 2010), major operation systems (McClure, 2008; Hatch, 2008) and ethical hacking (McClure, 2009; McClure et al., 2012). The topic of using web search engines for penetration tests is covered in *Google hacking* (Long, 2005) and the topic of denial of service attacks in *Framework for Classifying Denial of Service* (Hussain, 2003) and *Taxonomy of DDoS Attacks and DDoS Defense Mechanisms* (Mirkovic, 2010). All these books have been used as a background for Specific topics and Tools of PETA methodology.

Modern approaches to testing are presented in *CBEST Implementation guide* (CREST, 2014a) and *An introduction to CBEST* (CREST, 2014b), where is put a strong emphasis on threat intelligence (knowledge of tools and processes of attackers). Analysis of these approaches led the author to incorporate the threat intelligence as one of the areas of new methodology. Physical security is covered in *Two methodologies for physical penetration testing using social engineering* (Dimkov, 2009), malware testing in *A Framework for Malicious Workload Generation* (Sommers et al., 2004) and social engineering in *Social Engineering Your Employees to Information Security* (Manjak, 2006).

Reporting of penetration test results is covered in *Companies fail to fix system flaws uncovered by penetration testing* (Saran, 2004), *Using penetration testing feedback to cultivate an atmosphere of proactive security amongst end-users* (Styles, 2009) and *Writing a Penetration Testing Report* (Alharbi, 2010). Analysis of these sources was used for the creation of relevant part (reporting) of the detailed level.

More theoretical approaches can be found in Sun Tzu was a *Hacker: An Examination of the Tactics and Operations from a Real World Cyber Attack* (Rios, 2009), *Penetration Testing: Hacking Made Ethical to Test System Security* (Botenau, 2011) and *Moving toward black hat research in information systems security* (Mahmood et al., 2010). These sources were mainly used as an inspiration for the choice of the research topic.

Further we can mention publications that can be regarded as complementary – *Finding Bugs in Web Applications Using Dynamic Test Generation and Explicit-State Model Checking* (Artzi et al., 2010), *Improving CVSS-based vulnerability prioritization and response with context information* (Fruhwirth, 2009), *State of the Art: Automated Black-Box Web Application Vulnerability Testing* (Bau et al., 2010), *The impact of predicting attacker tools in security risk assessments* (Gutesman, 2010) and *Towards agile security assurance* (Beznosov et al., 2004).

4 Comparative analysis of current methodologies

In spite of the fact that penetration tests are a promising measure that could improve the current state of IS security, there are still some problems that usually lead to inferior results and in marginal cases even to IS functionality or availability disruption. Therefore, the preliminary research has been done during real world penetration tests on this subject by the author. Results from this preliminary research haven´t been published completely but are

mentioned in (Klima, 2014) and (Klima, 2015a). The following areas have been identified as most problematic:

1. Planning of penetration tests
2. Operational management of penetration tests
3. Implementation of countermeasures

The analysis of root cause (mainly consisted of interviews with penetration testers, security analysts, chief information officers and other employees involved in the problematics) of these problems showed that there is a lack of methodologies or frameworks useful for practical tests. Current methodologies and other available sources were also described as insufficient or missing important facts.

In order to identify areas which are not covered (or are covered insufficiently) in current methodologies, the comparative analysis has been conducted. In this analysis were included methodologies, which met the following criteria:

1. Have been published ten or fewer years ago
2. Are practically useful; pure theoretical approaches have been excluded
3. Are publicly available

These criteria were selected in order to ensure that methodologies included into scope aren´t obsolete (the literature review showed that ten years timeframe is a good dividing point between obsolete and current/usable sources), are useful for practical tests and the tester is able to obtain them without inadequate expenditures.

Based on the presented criteria the following methodologies were chosen: Open Source Security Testing Methodology Manual (Herzog, 2006), Information Systems Security Assessment Framework (OISSG, 2006), Penetration Testing Execution Stanard (PTES, 2015), OWASP methodology (OWASP, 2014) and NIST SP 800-115 standard (NIST, 2008).

The result of the comparative analysis is that current methodologies are not focused on management of penetration tests and aim primarily on the technical and high-level description of the testing process. Topics like the alignment of penetration test management with overall IT management/governance and project management of penetration tests are not discussed, which leads to bad planning, bad operational management of tests and unsystematic vulnerability remediation. Some of the methodologies (OISSG, 2006), (NIST, 2008) are also outdated and some have also a problem with practical usability (Herzog, 2006). Other aspects like complexity, tailoring possibilities or threat intelligence focus have been also analyzed. Results in graphical representation can be found in Table 1 (this table is reduced as the full table included in the methodology is too large to be shown in this article – 14 columns).

	Last revised	Focus			Tools	Easy to use	Integration to the context of IS/IT management
		Management	High level	Technical			
OSSTMM	2010	No	Yes	No	No	No	No
ISSAF	2006	Partially	Yes	Yes	Yes	No	Partially
PTES	2014	No	Yes	Yes	Yes	Yes	No
OWASP	2014	No	Yes	Yes	Yes	Yes	No
NIST SP 800-115	2008	No	Yes	No	No	Yes	No

***Tab. 1**. Comparative analysis of current methodologies. Source: author.*

5 PETA – new penetration testing methodology

In order to overcome above mentioned issues, the author has created the methodology named PETA which strives to be actual, complex and should have a tight connection with IT governance and IT security governance principles. This methodology is based on processes and principles of the classic methodologies mentioned above, but it contains up-to-date topics and uses principles of the COBIT and PRINCE2 frameworks. PETA has been in development since 2010 when the author had created the methodology WIPE (2010) for wireless network penetration testing. Afterward, WIPE methodology has been considerably extended in order to be useful for complex IS/IT penetration testing. PETA consists of the following layers:

- General level
- Detailed level
- Specific topics
- Tools

Basically, first two layers (general and detailed level) can be used in the long-term horizon without loss of accuracy. Two other layers (specific topics and tools) have to be updated regularly because IT security is a quickly changing field.

5.1 General level

The general level consists of two main areas – Incorporation of penetration tests into IT (security) management program and Project management of penetration tests.

5.1.1 Integration of penetration tests into context of IT management

Integration of penetration tests into IT management context is based on the process model from COBIT, which is tailored to suit the specific needs of penetration tests (an original model which contains 34 processes is reduced to 16 processes, see Figure 2). This reduced process model is an ideal baseline as the structure of the processes covers essential areas that can be effectively tested.

Every process from this model can be tested by one or more steps from the detailed level and one or more steps described in specific topics (relevant mapping table is too large to be included in the article). This reduced model is particularly useful for planning the tests

(decision which areas should be tested) and for remediation of vulnerabilities. In practice, the manager (usually chief information officer, chief information security officer or chief security officer) can easily benchmark security level of each process based on the results of penetration tests. He can also monitor the progress of remediation activities in specific areas. Assessment of specific processes or areas can be based on the metrics recommended by COBIT (Performance indicator/Outcome measure/Maturity model).

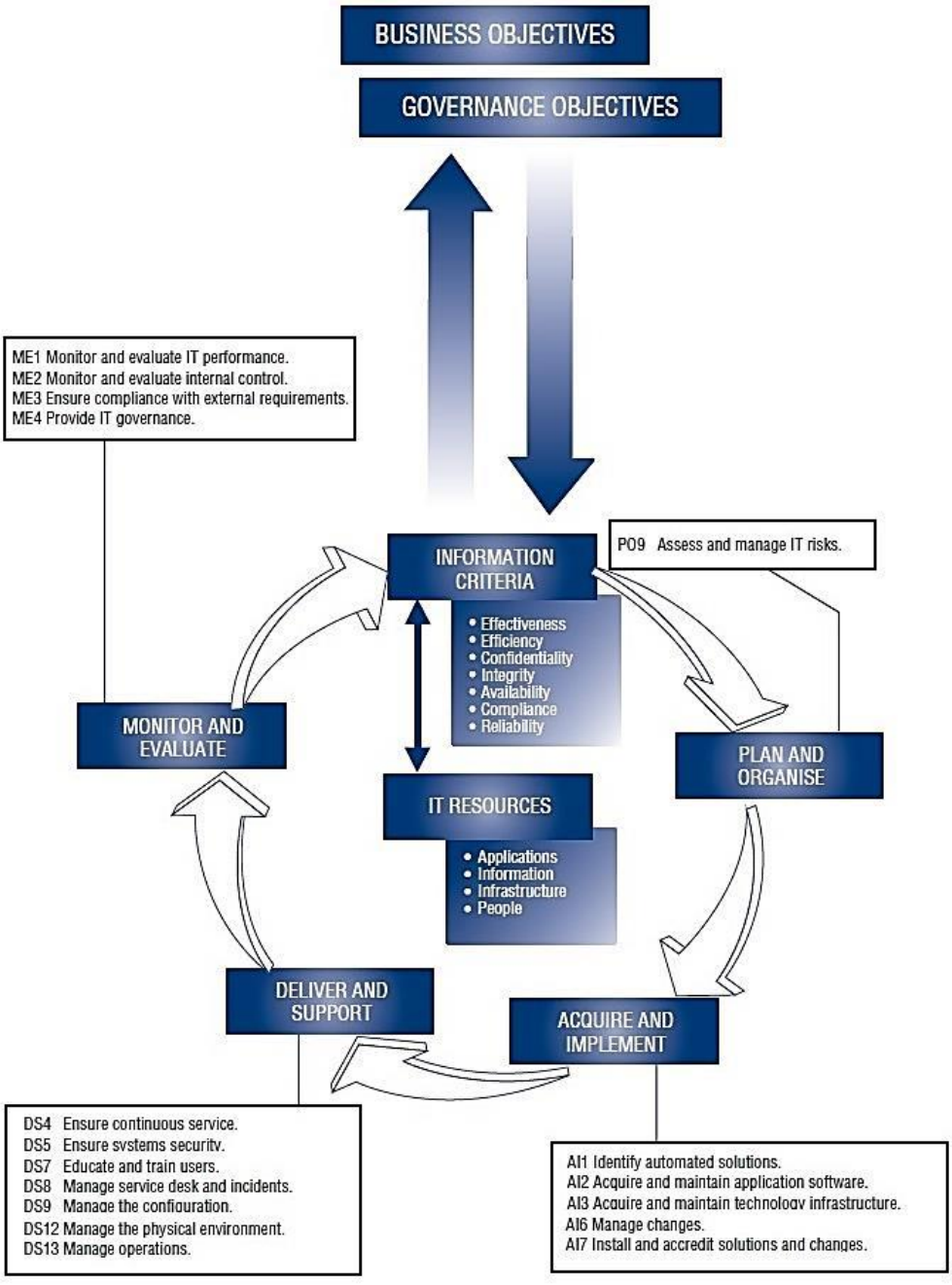

***Fig. 2**. COBIT - Reduced process model. Source: (ITGI, 2007), edited.*

5.1.2 Project management of penetration tests

Although every penetration test can be regarded as a project, current methodologies are not focused on this topic at all. Only in ISSAF (OISSG, 2006) are few basic principles covered.

This situation is remediated in PETA methodology which uses principles, themes and processes from PRINCE2 in order to set down basic rules. Again, only areas that suit specific needs of testing are incorporated. For example, we can name principles like Defined roles and responsibilities or Learn from experience, themes like Risk or Progress and processes like Controlling a stage and Managing stage boundary that was accordingly tailored. Another example of tailoring is the selection of relevant documents that should be created during complex penetration tests.

Previous lessons learned is a repository that should be updated with every project. Issues and their solutions should be kept here and reviewed with a start of every new project. During the project, the temporary lessons learned log should be created and after closing the project the final log should be saved into the repository. The test plan and description, the communication strategy, the team structure, roles and responsibilities can be described in separate documents, but it is a good practice to join them into one document called test plans and rules. Test plans can be designed according to the PRINCE2 principles and can have more levels of detail. But in all cases, they should have some milestones and deadlines set.

Test rules determine the tools and techniques that the tester is (un)authorized to use and how deep should the tester compromise the infrastructure. Other rules can be mutually agreed. The communication plan should contain all necessary contacts of team members and rules who should be contacted in case of problems. Also, there should be stated who is authorized to make decisions and who accepts the final report. Escalation procedures should be included too. Team structure, roles, and responsibilities is the document that includes the description of team roles, their duties and is closely connected with the communication strategy. The agreement is an optional document because in penetration tests conducted by in-house sources no such document is needed. In pentests conducted by an external company, an agreement is a basic (mandatory) document that should reflect all important points set in the test plan and description, communication strategy, team structure, roles and responsibilities.

The issue register should be used as a continuously updated repository in which issues that occurred during the test should be recorded. Also, the progress of the solution of these issues should be kept here. Pentester diary is a very important document that is recommended to every project regardless of its size because it enables the auditor to track the progress (and in the case of problems can help to identify the causes). Every step should be recorded with the exact timestamp, extracts from a command line and log files should be also included. In extreme cases (critical systems) the whole progress should be recorded by a desktop recording tool (like RecordMyDesktop in KALI Linux) or by a video cam recorder. Findings should be also continuously recorded by a pentester into a document with the same name. At the end of a pentest, the notes from this document are used to create the final report which is handed over to the management team for review and acceptance. This acceptance should be in the formal way (written document). Complete set of documents can be found in Figure 3.

5.2 Detailed level

On a detailed level, the processes that take place during a penetration test from the first touch with tested infrastructure to a complete compromise (if desired) are presented. Also, the work breakdown structure is introduced. See Table 2 to understand three basic steps (planning, testing and reporting) of the detailed level.

Planning	Testing	Reporting
1.1) Requirements identification	2.1) Information gathering	3.1) Cleanup
1.2) Stakeholder identification	2.2) Perimeter mapping	3.2) Document analysis
1.3) Project management team creation	2.3) Penetration	3.3) Report creation
1.4) Defining scope	2.4) Network scanning	3.4) Report presentation
1.5) Defining rules	2.5) Vulnerability scanning	
1.6) Testing team appointment	2.6) Penetration further	
1.7) Role description	2.7) Gaining access and escalation	
1.8) Kick off meeting	2.8) IS compromise	
	2.9) Maintaining access	
	2.10) Covering the tracks	

Tab. 2. *PETA – detailed level. Source: (Klima, 2015b).*

At first, during the planning step, the requirements for the test must be identified. Requirements can result from a need to adhere to some compliance standard (like PCI DSS), or a long-term security plan. Stakeholders and their needs must be also identified. Then the management team has to be created. This team appoints the testing team, no matter if the team is created from internal or external resources. The scope and rules are an important part of the test description and the test plan. The test description should include the tools and processes that the tester is (un)authorized to use and how deep should the tester compromise the infrastructure in case of successful penetration. The test is started by a kick-off meeting.

During the test, the auditor starts with the identification and the enumeration of publicly available information about the target organization. In this stage no contact with the target infrastructure is possible. When the satisfactory amount of information is gathered, the tester can start scanning and mapping the target network. From this moment, the tester can be detected by administrators and other staff of the client. After the mapping and the enumeration of the infrastructure the tester has knowledge of the network topology and running services and starts scanning for vulnerabilities that can result in the IS compromise. If the tester is successful in this step, he will try to escalate his privileges and maintain permanent access (usually creation of a new account or a new service). If it is required, the tester can hide his presence in the system and delete all relevant log files. After this stage, the tester should delete all the evidence like backdoors, temporary services, tools, and shares. After the test is over the auditor should analyze his notes and create a final report. After the acceptance of the final report, the test team should present this report to the management team. All steps described in this paragraph can be found in the graphical representation in Figure 3. Testers are expected to tailor this approach to meet the requirements of a specific test by adding or removing steps.

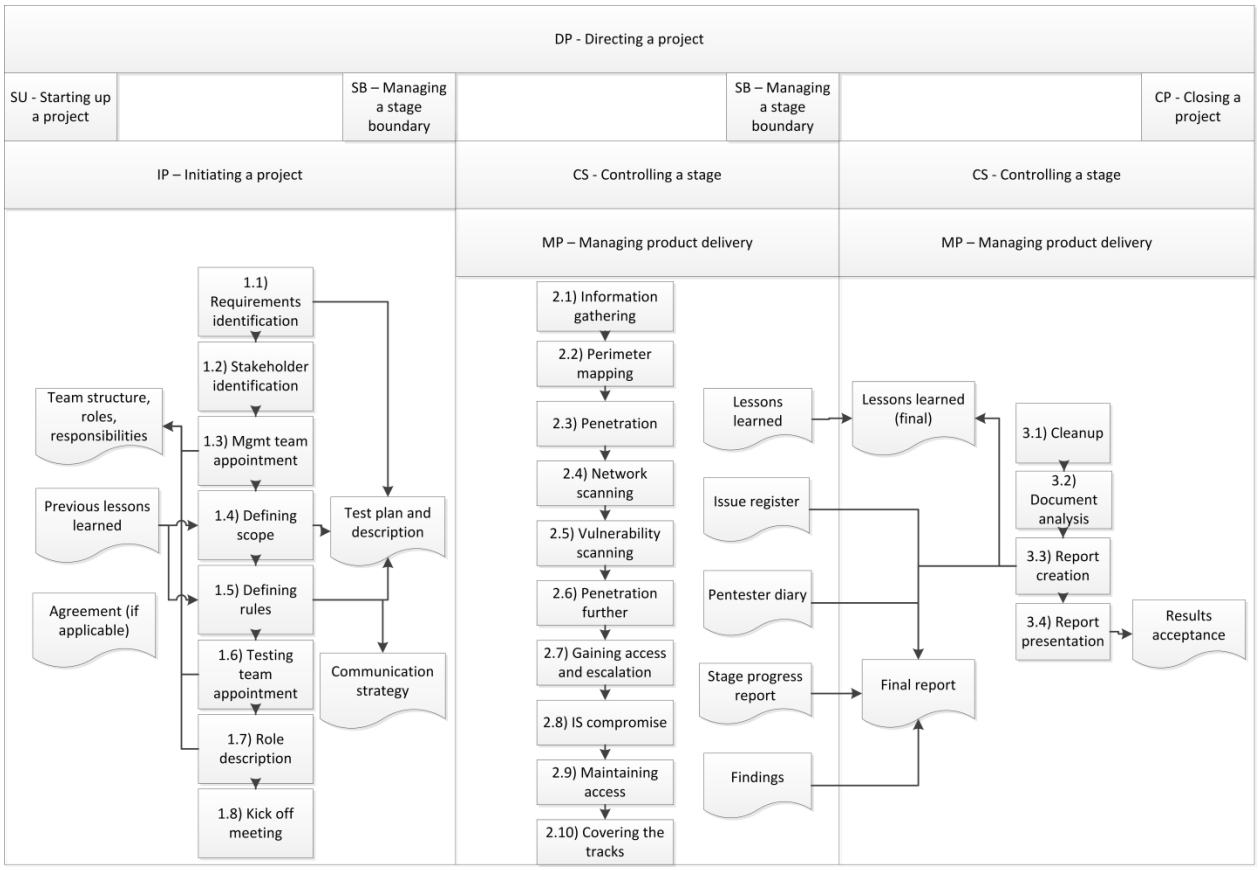

Fig. 3. *Process model. Source: (Klima, 2015b), edited.*

5.3 Specific topics

For exact tailoring, it is also necessary to select relevant specific topics from the Table 3 which cover areas that are commonly tested. Specifically, social engineering, DoS, incident response testing and mobile device testing are topics that aren´t commonly described in current methodologies. These topics (and also tools in the next section) are included in the methodology mainly for reasons of completeness, as the main focus of the methodology is on the management level.

Specific topics	**Abbreviation**
Web applications	WA
Web servers	WS
Social engineering	SI
Malware	MW
DoS, DDoS	DOS
Sniffing	SNI
Wireless networks	WI
Physical security	PS
Endpoint protection	EP
Incident response and detection testing	IR
Mobile devices	MD

Tab. 3. *PETA – specific topics. Source: (Klima, 2015b).*

5.4 Tools

In this section of the methodology are presented basic categories of tools that can be used during the test. Each category is enriched by a few examples of relevant tools and their usage. These categories are:

- Operation systems
- Information gathering tools
- Network scanners
- Vulnerability scanners
- Exploitation tools
- Backdoors
- Social engineering tools
- Password crackers
- Wireless networks testing tools
- Network sniffing tools
- Other tools

The tools presented should be sufficient for a complex penetration test. The testers are encouraged to use alternative methodology (for example PTES) for closer familiarization with presented tools.

6 Evaluation

Methodology PETA has been evaluated on the theoretical and practical level.

6.1 Theoretical evaluation

The theoretical evaluation consists of evidence that approaches to the management of penetration tests (including basic principles of the methodology) presented in PETA are not covered in current methodologies and thus are innovative. It extends the comparative analysis from the Section 4 of this article. Summarized results from the theoretical evaluation can be found in (comparative) Table 4, but key areas are discussed below.

Area of Integration to the context of IS/IT management can be partially found in ISSAF but only in connection with risk analysis. Practical usability is, unfortunately, limited. Other methodologies don´t deal with this topic at all. Compared to them PETA is primarily focused on the integration – reduced process model of COBIT is its first key part.

Project management of penetration test isn't described in a necessary level of detail in any of the current methodologies. The only exception is ISSAF where we can find topics like work breakdown structure, communication plan or risk management (in the context of the project). In PETA is project management considered as it's second key part.

Scalability, coverage (methodology covers all types of penetration tests) and ease of use are considered important principles in PETA. If we analyze other selected methodologies, we can see that only ISSAF and OWASP have functional scalable structure, OWASP and NIST 800-115 don´t have complete coverage of types of pentests and OSSTM and ISSAF aren´t easy to use. Threat analysis is partially described in current methodologies but only as an element of risk analysis. These methodologies, unfortunately, miss the concept of learning from the attacker´s tools and processes, which is discussed in PETA.

Other areas (technical level description, tools) are satisfactorily described in current methodologies.

Area	PETA	OSSTM	ISSAF	PTES	OWASP	NIST 800-115
Integration to the context of IS/IT management	Yes (primary focus)	No	Partially	No	No	No
Project management of penetration tests	Yes (primary focus)	No	Partially	No	No	No
Technical level description	Partially	No	Yes	Yes	Yes	No
Tools	Partially	No	Yes	Yes	Yes	No
Scalability	Yes	Partially	Yes	Partially	Yes	Partially
Coverage	Yes	Yes	Yes	Yes	No	No
Easy of use	Yes	No	No	Yes	Yes	Yes
Threat analysis	Yes (updated and extended)	Partially	Partially	Yes	Partially	No

Tab. 4. *Theoretical evaluation. Source: author.*

Author´s publications can be considered as the second part of the theoretical evaluation. The question of integration into the context of IS/IT management was discussed in (Klima, 2014). The topic of project management of penetration tests was analyzed in (Klíma, 2015a) and (Klima & Tománek, 2015). The whole methodology was presented on the conference IT in Central Banks forum (Klima, 2015b).

Theoretical evaluation can be considered as confirmation that new methodology fills the gaps that had been identified in the comparative analysis of current methodologies (and that relevant parts of the methodology have been successfully peer reviewed). In order to prove that new methodology is practically usable and has benefits in comparison with current approaches, practical evaluation has also been conducted.

6.2 Practical evaluation

Practical evaluation (case study) consists of six real-world penetration tests (main group) that were managed according to the PETA methodology and their comparison with two tests that were managed according to other approaches (control group). All of these tests were conducted in the target company, which belongs to the banking sector and has 1000+ employees. In order to protect an identity of the organizations, more details can´t be disclosed. A quantitative approach is employed during the evaluation.

6.2.1 Main group

1) LAN network penetration test (2012)

The first penetration test was focused on the security of the internal network. This test was grey-box (partial knowledge of the infrastructure) and the administrators were not aware that test is taking place. PETA was used for planning, operational management and implementation of countermeasures with a strong focus on proper project management. Tester was outsourced from an external company. For technical testing processes, he employed his own methodology, which was used in tandem with PETA. Selected relevant processes from the reduced process model were PO9, AI1, AI2, AI3, AI6, AI7, DS4, DS5, DS8, DS9, DS13, ME2 (see Figure 2).

During the test, after the reconnaissance phase, a number of servers were compromised and the tester achieved elevated privileges which gave him partial control of the network. The administrators were successful in detection and identification of the tester´s activities, which proved their good monitoring abilities.

All the vulnerabilities were assigned to a relevant COBIT processes and remediated.

2) Wireless networks penetration test (2014)

The second test was conducted in order to evaluate the security of company´s wireless networks. The whole test was conducted according to PETA methodology (detailed technical steps were used from ISSAF and PTES). Selected relevant processes from the reduced process model were PO9, AI3, AI6, DS4, DS5, DS9 (see Figure 2).

The test was conducted by internal employees, the approach was white-box (knowledge of network topology and other information). Administrators were aware of the test.

After the mapping of the coverage of the wireless signal, the tester penetrated into the selected network, sniffed the traffic with knowledge of the shared password and compromised a wireless router where he achieved administrator privileges. Besides the identification of vulnerabilities, the benefit was also the simulation of the situation when the external attacker has wireless access point under his control and can manipulate the traffic.

Findings from this tests resulted in a redesign of wireless networks in the organization.

3) Social engineering penetration test (2014)

The third test was focused mainly on the human element of the IT security – it tested user awareness and ability to identify malicious email. In combination with phishing campaign it also verified the level of technical means of defense – spam filter and antivirus software. The phishing campaign, which was the primary tool of this test, was planned and prepared in cooperation with the external company. PETA was used for planning, operational management and implementation of countermeasures. The COBIT process model was used for proper focusing of the test. Relevant processes from the reduced process model were PO9, AI1, AI2, DS5, DS7, DS8, DS9, ME2 (see Figure 2).

The test consisted of three phases. In the first phase, a batch of testing emails with the malicious link was send. The reaction of users (number of users who clicked this link and number of users who reported an incident) was then analyzed. After that, the seminar about cyber-threats connected to phishing was prepared. In the timeframe of one month, the test was repeated in order to verify the efficiency of the seminar.

The results of this test led to a creation of the user awareness program in the target company.

4) Filing service IS penetration test (2014)

This test was planned and prepared by the internal employees but was executed by outsourced testers, who had their own methodology for detailed testing processes. PETA was used for planning and implementation of countermeasures. Relevant processes from the reduced process model were PO9, AI1, AI2, AI3, AI6, AI7, DS4, DS5, DS9, ME2 (see Figure 2). The test was white-box and administrators were aware of it. The goal of the test was to evaluate the security of the Filing service information system before it was accepted into the production environment.

The practical tests were focused on web application and web server and were complemented by a proper security audit of the configuration of the application server and operation systems running on the tested servers.

The vulnerabilities found were properly remediated and the information system was approved for a production environment.

5) Banking IS penetration test (2015)

In order to comply with a regulation (intentionally the specific regulatory act/standard is not mentioned in order to protect the identity of the target organization), the penetration test of Banking IS had to be done. The test was conducted by outsourced testers and managed according to PETA, which was used for planning, operational management and implementation of countermeasures, again with a strong focus on project management and proper documentation. Relevant processes from the reduced process model were the same as in the previous test. The test was grey-box, without knowledge of the application source code. All relevant employees were aware that the test was taking place.

During the test, the main focus was on the web application, but also web server was audited. A number of vulnerabilities were identified and these vulnerabilities were remediated in a timely fashion. This test resulted in improvement of company secure software development lifecycle.

Management of this test and the remediation of the vulnerabilities were evaluated by an internal audit division during an audit task. The final report graded the examined areas as "excellent".

6) Management network for Johnson Controls (2015)

As this part of the company network was a concern for the management of IT security division, it was decided to audit it according to the PETA methodology. The whole test was managed according to PETA methodology and was conducted by internal employees. Selected relevant processes from the reduced process model were PO9, AI3, AI6, AI7, DS4, DS5, DS9, ME2 (see Figure 2).

The first step was a mapping of the network, which was followed by an identification of the vulnerabilities (mainly caused by misconfiguration of the devices). According to the test rules, these vulnerabilities were used for a compromise of target devices. No further movement in infrastructure was allowed so the test ended with an administrator access to a group of target devices.

This test resulted in a redesign of tested part of the network and its separation from the internal network. In 2016 tests of other five information systems are planned and PETA will be used as a methodology for their management.

6.2.2 Control group

As the control group were selected penetration tests conducted according to the in-house methodology of the target organization or by an approach based on the experience of the project manager in combination with vendor´s methodologies. The control group contains:

1) E-banking penetration test (2006)

This test was performed by an external company which used its own methodology. The goal of the tests was to evaluate the security of the target system before its deployment into a production environment. Management of the test was based on the experience and tacit knowledge of the project manager. The vulnerabilities were mainly found on the database level but the missing operational level practices led to closely unspecified incidents (these incidents had no impact on functionality or availability of the target system).

2) External penetration test (2013)

This test was conducted as a simulation of cyber-attack from the internet with a goal to penetrate the company perimeter. The test was performed by an external company which used its own methodology for the whole (black-box) test and was managed according to the in-house methodology of the target organization. Administrators were informed about the exact date of the test. The only document prepared was the agreement and the final report.

Only low-risk vulnerabilities were found and overall benefit for the tested infrastructure was low.

6.2.3 Results

Because the focus of PETA is on the management of penetration tests, common metrics like total number of (serious) vulnerabilities found, the number of (serious) vulnerabilities per device, the number of tested devices/total number of devices or CVSS (Common Vulnerability Scoring System) score of vulnerabilities found are unusable for determining the difference in quality of tests between the two comparison groups. Therefore, the evaluation had been done by a quantitative method employing the questionnaires, which were filled out by stakeholders. In the target company were identified two managers who were involved in the majority of evaluated tests. The first is the Information technology security manager (involved in all of the tests) and the second is the Information technology operations manager (involved in all of the tests except the Management network for Johnson Controls penetration tests).

In the questionnaire were represented all eight penetration tests in chronological order and for each test the stakeholders had to evaluate the following criteria on a scale 1-10 (higher number means higher rating, only in Impact on tested systems higher number means higher (negative) impact on functionality or availability).

1) Overall benefit of a penetration test.
2) Quality of planning.
3) Quality of operational management.
4) Quality of implementation of countermeasures.
5) Quality of documentation.
6) Impact on tested systems.

For each group of the penetration tests (main and control) was then an average computed for each of the six criteria (separately for each evaluator). The difference between the average of main group and control group (for each criterion) was then computed according to the following formula:

$$x = \frac{\sum_1^m a_i}{m} - \frac{\sum_1^n b_j}{n} \quad (1)$$

x = diffence in average score for given criterion

a_i = value of each individual score from main group

b_j = value of each individual score from control group

n, m = number of items being averaged

The results, which we can see in Table 5, show that:

1) In all of the criteria, the tests managed according to PETA have better results than the tests in the control group.
2) The mean (average) difference in the Overall benefit of a penetration test is higher in the main group by 2,57 in comparison to control group.
3) The biggest mean difference we can see in the evaluation of Quality of planning (4,05).
4) The shift in a score of Quality of documentation (2,5) and Quality of operational management (2,24) can be considered as significant, but not so high as in the previous criterion.
5) Lowest shift was noticed in the evaluation of Quality of implementation of countermeasures (1,62).
6) The impact on tested systems was evaluated as negligible in all of the tests, therefore this criterion can be omitted.

		IT security manager			**IT operations manager**			**Mean diff**
		PETA	ctrl. group	**diff**	PETA	ctrl. group	**diff**	
1)	Overall benefit of penetration test	8,83	6,00	**2,83**	9,80	7,50	**2,30**	**2,57**
2)	Quality of planning	8,50	5,00	**3,50**	9,60	5, 00	**4,60**	**4,05**
3)	Quality of operational management	8,17	6,50	**1,67**	9,80	7,00	**2,80**	**2,24**
4)	Quality of implementation of countermeasures	7,83	7,00	**0,83**	9,40	7, 00	**2,40**	**1,62**
5)	Quality of documentation	9,00	5,50	**3,50**	9,00	7,50	**1,50**	**2,5**
6)	Impact on tested systems	1,00	1,00	**0,00**	1,00	1,00	**0,00**	**0,00**

Tab. 5. *Practical evaluation. Source: author.*

If we omit the Impact on the tested systems, we can compute the average difference of the rest of the criteria. Based on the numbers presented in Table 5, the value of the average difference is 2,6 (sum of the mean differences in the last column/number of items). This number tells us that the average evaluation of the tests managed according PETA was by 2,6 points higher (on a ten-point scale) in comparison to the control group.

7 Discussion

Current approaches to penetration testing mainly consist of a high level and technical description of the testing process (some of them also deal with a usage of tools). This was proven by the comparative analysis of current methodologies and literature review in the first part of the article. Description of the management level is missing and therefore the organizations are forced to create in-house methodologies or adopt vendor´s methodologies (which are, in fact, also in-house).

Methodology PETA covers this missing management level and, as was proven in the theoretical part of the evaluation, focuses on the areas that were not described before. These areas are Integration to the context of IS/IT management, Project management of penetration test and Threat analysis. Furthermore, the coverage of the methodology is complete, which means it is usable for all types of penetration tests.

In order to prove practical usability, PETA has been used for the management of six penetration tests between 2012 and 2015. Results of these tests were compared to the results of two penetration tests that were managed according to the internal methodology of the target organization or an approach based on the experience of the project manager (in combination with vendor´s methodologies, where relevant). As the quantitative metrics commonly used in this area are unsuitable, the difference in overall benefit, quality of planning, operational management, implementation, and documentation as well as the impact on the tested system was evaluated by the questionnaires filled out by the involved stakeholders (IT security manager, IT operations manager).

These results show that the tests managed according to the PETA were evaluated as superior to tests in the control group (tests managed by other approaches) in five of the six criteria (the sixth criterion was omitted as the impact on tested systems was negligible in all of the tests). The biggest difference we can see in the evaluation of Quality of planning (4,05), whereas the difference in evaluation of Quality of documentation (2,5) and Quality of operational management (2,24) can be seen as a medium, but still significant. The lowest improvement was noticed in the evaluation of Quality of implementation of countermeasures (1,62). The most important criterion, the Overall benefit of a penetration test, was evaluated as higher by 2,57 in comparison to control group.

On limited sample was therefore proven that new methodology is usable for practical tests and is able to deliver better results than current approaches. The PETA methodology was also reviewed by the employees of internal audit division of target organization and was recommended for internal use as an official methodology for management of penetration tests.

8 Conclusion and further research

In spite of the fact that penetration tests are used for the assessment of IS security from the late sixties (in a commercial sphere from the nineties), there is no single standard, methodology or framework that is both practically usable and covers all aspects of these tests. Testers, therefore, use various methodologies mentioned earlier in this article in combination with in-house methodologies (and their tacit knowledge). The outputs from the tests aren´t thus easily comparable and their benefit for the overall security level of the tested systems is suboptimal.

In this article was presented methodology PETA, which covers missing approaches to the management of penetration tests. The methodology has been theoretically and practically evaluated on a limited sample of six penetration tests. It was proven by quantitative means that these six tests were perceived as superior in five out of six evaluated criteria to control group of two penetration tests managed by other approaches (the sixth criterion was omitted, as described above). The methodology was also recommended for internal use by the internal audit division of the target organization.

Further improvement will be mainly focused on the integration of PETA into some existing standard. Preferred is Penetration Testing Execution Standard (PTES, 2015), which is periodically updated and offers a detailed description of testing processes.

References

Alharbi, M. (2010). Writing a Penetration Testing Report. *SANS Institute*. Retrieved from: http://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343

Artzi, S., Kiezun, A., & Dolby, J. (2010). Finding Bugs in Web Applications Using Dynamic Test Generation and Explicit-State Model Checking. *IEEE Transactions on Software Engineering*, 36(4), 474-494. doi: 10.1109/TSE.2010.31

Bau, J., Butsztein, E., Gupta, D., & Mitchell, J. (2010). State of the Art: Automated Black-Box Web Application Vulnerability Testing. In *Proceedings of the IEEE Symposium on Security and Privacy*, (pp. 332-345). New York: IEEE. doi: 10.1109/SP.2010.27

Beznosov, K., & Kruchten, P., Yu, H. (2004). *Towards agile security assurance*. In Proceedings of the workshop on new security paradigms. New York: ACM Press. doi: 10.1145/1065907.1066034

Botenau, D. (2011). Penetration Testing: Hacking Made Ethical to Test System Security. *Canadian Manager*, 36(3), 10-11.

BSI (2008). A penetration testing model. *Federal office for information security*. Retrieved from: https://www.bsi.bund.de/EN/Publications/publications_node.html

Cache, J., & Liu, V. (2007) *Hacking exposed wireless: wireless security secrets & solutions*. New York: McGraw-Hill.

CheckPoint (2013). Check Point 2013 security report. Retrieved from: https://www.checkpoint.com/security-report/

CREST (2014a). CBEST Implementation Guide. Retrieved from: http://www.crest-approved.org/wp-content/uploads/CBEST-Implementation-Guide.pdf

CREST (2014b). An introduction to CBEST. Retrieved from: http://www.crest-approved.org/wp-content/uploads/CBEST-OVERVIEW.pdf

Davis, M., & Bodmer, S. (2010). *Hacking exposed malware & rootkits: malware & rootkits security secrets & solutions*. New York: McGraw-Hill.

Dimov, T. (2009). *Two methodologies for physical penetration testing using social engineering.* Technical Report TR-CTIT-09-48. Enschede: Centre for Telematics and Information Technology University of Twente.

Doucek, P., Novák, L., Nedomová, L., & Svatá, V. (2011). *Řízení bezpečnosti informací*. Praha: Professional Publishing.

EC-COUNCIL (2011). *Ethical hacking and countermeasures v7.1.*

Farmer, D. & Venema, W. (1993). *Improving the Security of Your Site by Breaking Into it*. Retrieved from: http://www.fish2.com/security/admin-guide-to-cracking.html

Fruhwirt, C., & Mannisto, T. (2009). *Improving CVSS-based vulnerability prioritization and response with context information.* In *Proceedings of the 3rd International Symposium on Empirical Software Engineering and Measurement*, (pp. 535-544). New York: IEEE. doi: 10.1109/ESEM.2009.5314230

Hatch, B. (2008). *Hacking exposed Linux: Linux security secrets & solutions*. 3rd ed. New York: McGraw-Hill.

Herzog, P. (2006). *Open-Source Security Testing Methodology Manual.* Catalonia: ISECOM.

Hussain, A. (2003). A Framework for Classifying Denial of Service. In *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, (pp. 99-110). New York: ACM. doi: 10.1145/863955.863968

Information security forum (2007). *The standard of good practice for information security*. London: Information security forum.

ISACA (2004). *IS Auditing procedure: Security assessment – penetration testing and vulnerability analysis.* Rolling Meadows: ISACA.

ITGI (2007). *Cobit 4.1*. Rolling Meadows: IT Governance Institute.

ITGI (2008). *Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit*. Rolling Meadows: IT Governance Institute.

ITGI (2012). *Cobit 5*. Rolling Meadows: IT Governance Institute.

Klíma, T. (2010). *Wireless networks security assessment.* Master's thesis. Prague: University of Economics, Prague.

Klíma, T. (2014). Využití metodiky COBIT 4.1 při penetračním testování bezpečnosti IS. In *Sborník prací vědeckého semináře doktorského studia FIS VŠE,* (pp. 43-49). Praha: Oeconomica.

Klíma, T. (2015a) Projektové řízení penetračních testů IS. In *Sborník prací vědeckého semináře doktorského studia FIS VŠE*, (pp. 41-48). Praha: Oeconomica.

Klíma, T. (2015b). *Management of information systems penetration tests* [presentation]. IT in Central Banks Forum. Serbia.

Klíma, T., & Tománek, M. (2015). Project Management of Complex Penetration Tests. In: *Proceedings of the 14th European Conference on Cyber Warfare and Security ECCWS-2015*, (pp. 383-388). Reading: ACPI.

Koster, J. (2012). *In-house Penetration Testing for PCI DSS*. Retrieved from: http://www.sans.org/reading-room/whitepapers/compliance/in-house-penetration-testing-pci-dss-33930

Long, J. (2005). *Google hacking*. Brno: Zoner Press.

Mahmood, M., Siponen, M., Straub, D., Rao, R. H., & Raghu, T. S. (2010). Moving Toward Black Hat Research in Information Systems Security: An Editorial Introduction to the Special Issue. *MIS Quarterly,* 34(3), 431-433.

Manjak, M. (2006). Social Engineering Your Employees to Information Security. *SANS Institute*. Retrieved from: http://www.sans.org/reading-room/whitepapers/engineering/social-engineering-employees-information-security-1686

Mirkovic, J., & Reiher, P. (2010). A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2), 39-53. doi: 10.1145/997150.997156

NIST (2008). *Technical Guide to Information Security Testing and Assessment: NIST Special Publication 800-115*. Gaithersburg: National Institute of Standards and Technology.

NIST (2013). *Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800 - 53*. Gaithersburg: National Institute of Standards and Technology. Retrieved from: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Northcutt, S. (2006) *Penetration Testing: Assessing Your Overall Security Before Attackers Do*. *SANS Institute*. Retrieved from: https://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635

Office of Government Commerce (2009) *Managing successful projects with Prince2*. 5th ed. London: TSO.

OISSG (2006). *Information systems security assessment framework.* Open information systems security group.

OWASP (2014). OWASP testing guide 4.0. Retrieved from: https://www.owasp.org/images/5/52/OWASP_Testing_Guide_v4.pdf

PCI Security standards council (2008). PCI DSS: Information Supplement: Requirement 11.3 Penetration Testing.

Pereira, T. & Santos, H. (2010). A Conceptual Model Approach to Manage and Audit Information Systems Security. In *Proceedings of the 9th European Conference on Information Warfare and Security*, (pp. 360-365). Reading: ACPI.

PTES (2015). Penetration Testing Execution Standard. Retrieved from: http:// http://www.pentest-standard.org/

Rios, B. (2009). Sun Tzu was a Hacker: An Examination of the Tactics and Operations from a Real World Cyber Attack. Retrieved from: https://ccdcoe.org/publications/virtualbattlefield/10_RIOS_Sun_Tzu_was_a_hacker.pdf

SANS (2010). *Penetration testing in the financial services industry. SANS Institute*. Retrieved from: https://www.sans.org/reading-room/whitepapers/testing/penetration-testing-financial-services-industry-33314

SANS (2014). The Critical Security Controls for Effective Cyber Defense. *SANS Institute*. Retrieved from: https://www.sans.org/media/critical-security-controls/CSC-5.pdf

Saran, C. (2004) Companies fail to fix system flaws uncovered by penetration testing. *Computer Weekly*. Retrieved from: http://www.computerweekly.com/news/2240056864/Companies-fail-to-fix-system-flaws-uncovered-by-penetration-testing

Scambray, J., & McClure, S. (2008) *Hacking exposed Windows: Windows security secrets & solutions*. 3rd ed. New York: McGraw-Hill.

McClure, S. (2009). *Hacking exposed*. New York: McGraw-Hill.

McClure, S., Scambray, J., & Kurtz, G. (2012) *Hacking exposed 7: network security secrets & solutions*. New York: McGraw-Hill Education.

Styles, M., & Trynofas, T. (2009). Using penetration testing feedback to cultivate an atmosphere of proactive security amongst end-users. *Information Management & Computer Security*. 17(1), 44-52. doi: 10.1108/09685220910944759

Sommers, J., Yegneswaran, V., & Barford, P. (2004). A framework for malicious workload generation. In *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*. New York: ACM Press. doi: 10.1145/1028788.1028799

Suduc, A., Bizoi, M., & Filip, F. (2010) Audit for Information Systems Security. *Informatica Economica*, 14(1), 43-48.

Swanson, M. (1996). Generally Accepted Principles and Practices for Securing Information Technology Systems: NIST Special Publication 800-14. *NIST Institute*. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

Veenendaal, V. (2012). Test maturity model integration (TMMi). *TMMI Foundation*. Retrieved from: http://www.tmmi.org/?q=downloads

Verizon (2013). *Data breach investigations report.* New York: Verizon.

Verizon (2015). *Data breach investigations report*. New York: Verizon.

Wai, C. (2002). Conducting a Penetration Test on an Organization. *SANS Institute*. Retrieved from: http://www.sans.org/reading-room/whitepapers/auditing/conducting-penetration-test-organization-67