Towards a Social Engineering Test Framework

David Kelm and Melanie Volkamer

CASED, TU Darmstadt, Hochschulstr. 10, 64289, Darmstadt, Germany

Abstract. A growing number of hacking attacks use social engineering techniques to exploit the *human factor* of computer systems. They include versatile sophisticated approaches like reciprocity, authority or manipulation techniques to capitalize on in general positives of humans such as helpfulness. These attacking techniques are used in the private as well as in the business context. In the latter they form a main tool for industrial espionage. While there exist evaluation standards for security critical software and hardware as well as their operational environment, due to our knowledge there is no evaluation standard available in order to evaluate vulnerability of organizations with respect to social engineering. This paper will present a framework to evaluate this kind of vulnerability. This framework includes whitebox as well as blackbox tests. The framework enables organizations to elaborate the level of resistance as well as to identify concrete vulnerabilities. These can be used to implement concrete measures to improve the situation, i.e. the level of resistance.

1 Introduction

Breaches in security often elude our ability to defend against and thus lead to billions of dollars annually in individual and corporate losses [14]. One major problem in this connection is industrial espionage. Thereby, attackers gain access to sensitive data and information by abusing technical or human vulnerabilities. The human vulnerabilities build one of the most hazardous information security threats since, according to the *Information Security Handbook: A Guide for Managers* of the National Institute of Standards and Technology (NIST), "people are arguably the weakest element in the security formula that is used to secure systems and networks" [1]. Thus, the "people factor", a critical factor, which is often overlooked, provides massive opportunities for security improvements in order to protect business properties.

We focus here on the human vulnerability, which is exploited by *social engineering*. Social engineering is according to Christopher Hadnagy [7], the "Art of Human Hacking" i.e. manipulating people into performing actions, which enables adversaries to gather information and exploit vulnerabilities.

Social engineering often starts with information gathering where the social engineer tries to collect as much information as she can, for example by searching through dumpsters or conducting a simple google search. By means of the gathered ‘public’ information she plans next steps. Here she attempts to develop a relationship with her victim to exploit an awareness deficit and insufficient security skills, usually

Kelm D. and Volkamer M..
Towards a Social Engineering Test Framework.
DOI: 10.5220/0004980000380048
In *Proceedings of the 11th International Workshop on Security in Information Systems* (WOSIS-2014), pages 38-48
ISBN: 978-989-758-031-4

by utilizing techniques such as impersonation and manipulation. Thereby, adversaries abuse human natural behavior and characteristics such as helpfulness, curiosity, credulity, kindness or authority hearing.

Since, due to our knowledge, there exist only frameworks to evaluate how resistant infrastructures of organizations are against technical hacks, but not against social engineering attacks our main aim is to provide a *social engineering test framework*. It consists of three stages: gather information, exploit information and a document and interview based analysis. The framework provides advice to auditors conducting the evaluation. This includes what type of information should be tried to gather as well as how it could be used for social engineering attacks. Additionally, it contains information about the type of documents to be reviewed and the questions that should be addressed in the interviews. Furthermore, the framework is designed in a way that after the evaluation and determined vulnerability level a written report is handed out.

2 Related Work

There are plenty of standards dealing with the topic of organizational security tests, albeit the present literature seldom addresses the measurement of social engineering. The ISO27000 series of standards have been specifically reserved by the International Organization for Standardization (ISO) for information security matters. Therefore, many modules are defined that try to list some best practices recommendations. Despite the fact that these are huge documents with an enormous scope, this series addresses social engineering just marginally. Just ISO27005 offers more details when it comes to Risk assessment. Nevertheless, it offers no specific risk analysis methods. In contrast to ISO27000 security testing, the proposed social engineering test framework is not aimed to emit certificates, but to measure the specific vulnerability of social engineering. Therefore, the organization under test will get an assessment with respect to social engineering.

In [9] the authors offer a metric for risk assessment. However, they just rely on experiments with employees and execute one test. To get a realistic overview about the security of a company we propose to conduct several different experiments and an additional internal observation. [12] also gives some hints about conducting social engineering penetration tests, but leaves still a lot of open questions and stays vague. Nevertheless, a significant point that is mentioned here is e.g. the ethical component of social engineering penetration tests.

As input for the development of our social engineering test framework, we also studied general security test literature: In (Smith and Shorter, 2010, pp. 358-363) the authors compare white box and black box penetration tests and conclude that both kinds of tests should be conducted. Thus, we cover both parts within our recommendations for social engineering penetration tests.

Moreover, Pierce et al., [13] critically reviewed seven penetration testing methodologies in practice, considering the commercial environment, open source frameworks and the literature. Similar characteristics were observed among the methodologies, such as progressive frameworks and similar concepts were reflected in the phases part of testing. The survey identified five major phases of testing:

reconnaissance, planning, penetration, escape and documentation. Penetration and planning are considered to be the two main issues for successful rigorous penetration testing and will be focused on within this paper as well. In contrast, classical penetration tests as the Open-Source Security Testing Methodology Manual (OSSTMM) [10] mention social engineering, but do not provide tests. In [5], the German Federal Office for Information Security (BSI) points out a structured methodology for penetration tests based on OSSTMM. However, it does only provide an overview and some assistance to approach a general testing concept well structured.

3 Framework Overview

The aim of this section is to propose and overview of the social engineering test framework (visualized in Fig. 1). We propose to begin as a real social engineer would do, to achieve a realistic testing approach. That is, by verifying what kind of information can be gathered about the organization under evaluation and chooses our 'penetration' test scenarios based on the respective results. i.e. gathered information.

The framework is divided into an external and an internal part. In the *external* part the auditor has no insight into the organization's internal structure. As such black box tests are conducted, within which information gathering and its exploitation by real attacks is done. During the *internal analysis*, the current policies and security culture (based on interviews) are evaluated. Hence a document based white box test is conducted.

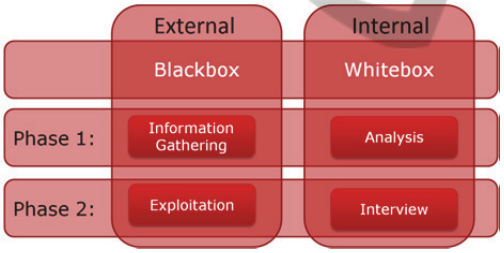

Fig. 1. Visualization of the stages of the social engineering test framework.

It is possible to conduct the external and the internal stage simultaneously. But, then the auditor for both stages should not be the same person, since the auditor may use internal information for her attacking scenarios, even if unintentionally.

General Remarks: Before any tests are executed, it is important that possible conflicts with the staff association and the organizations' chief officers are clarified. Especially in the case of compliance or skill and awareness checks, these tests can cause problems in the juristic field of employee observation. As a matter of course, the organization has to define a clear scope and rules of engagement for testing. The scope should include, at a minimum, systems with the organization's highest value information and production processing functionality.

4 Blackbox Testing

Within the blackbox tests the auditor initially gathers information, based on a checklist that is provided as part of the proposed framework. This checklist is derived from a broad literature review, e.g. [11], [8], [4], [2], and [7]. Depending on the list and type of information that could be gathered, appropriate and possible attacking scenarios are deduced. Therefore, the framework provides a large list of attacking scenarios as well as an algorithm supporting the auditor to select attacking scenarios. The selected attacking scenarios are executed in the second phase.

4.1 Phase 1: Information Gathering

We start with information gathering from publically available sources to follow the track of a malicious social engineer. Within this phase of the evaluation, we measure to what extent information about the organization can be collected, i.e. about the degree to which the organization is either robust or prone to social engineering attacks. It bases upon the fact that, if more information can be found, more sophisticated attacks are possible. Depending on the degree of information gathering approved by the organization under test, also a collection of public contact information can be executed as a part of this check. Due to financial or time constraints, some organizations may want to limit this phase; therefore e.g. the employees' contact information can be handed out to the auditor in order to conduct the attacks in the next phase (of e.g. phishing attacks).

Our framework offers assistance in information gathering by means of a checklist with 39 items. We first describe the frameworks' information gathering checklist before we explain how it is used within Phase 1.

4.1.1 Information Gathering Checklist

To develop this checklist, we collected information about occurred and publicly known social engineering incidents e.g. [11], [8], [4], [2], [7] and searched for proposed tactics e.g. [7] or [12]. We evaluated which information abets social engineering attacks and how critical they may be. Included checklist-items indicate how well informed an attacker can be, when she conducts serious information gathering. In order to rate and rank the results of phase 1, risk values are assigned for each item. These risk values depend on the number of possible attacks and the exploitation risk that they pose to an organization. The checklist could not be included in the paper due to space limitations.

4.1.2 Usage of the Information Gathering Checklist

If within an extensive information gathering search an information item is found, the corresponding risk value is added to the total value. Therefore, four values are assigned from 1 (not critical) to 4 (extremely critical). Since it is very important how easily an attacker can gather this information, the auditor additionally defines how

easily she achieved this information and classifies the effort. The corresponding algorithm is pictured in Figure 2 a). Hence another five values can be assigned: 0 (no information found), 1 (by physical), 2 (via phone), 3 (via internet) and x (not tried to find this information).

To rank these findings, the values of the found items' risk value are summed up, while the average effort value is calculated. As a matter of fact the average effort value (of our 39 items) should be as low as possible (since a low effort value means more effort had to be invested to collect the corresponding information). We estimate that an average effort value below 1.2 should be desirable (note, this need to be confirmed by case studies applying this framework). By means of this checklist, a maximum cumulated risk value of 345 can be achieved.

Additionally, we define a maximum possible value since information the researcher was not looking for should not influence the results in a positive way: meant is the maximum value excluding all *x-values*. Due to the fact that a lower value illustrates a better immunity against information gathering we propose the following assessment: A value lower than 1/7 of the maximum possible value seems to be fine, lower than 1/4 is still ok while an value between 1/4 and 1/2 of the maximum possible value is critical. If more than 1/2 of the maximum possible critical value is reached, a very high risk should be considered. Since these values are just an estimated proposal point of reference, they need to be empirically verified in future within a case study.

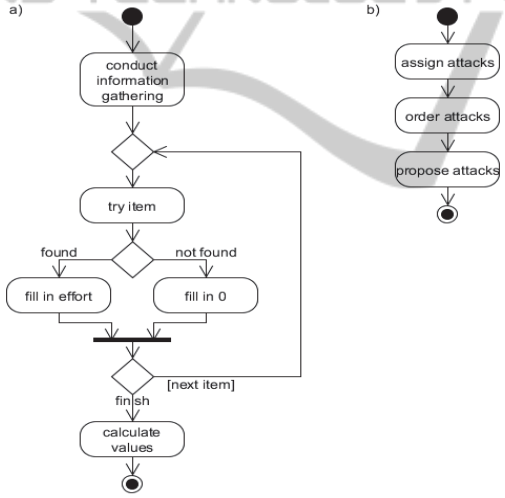

Fig. 2. a) Algorithm for information gathering. b) Algorithm for assigning and proposing attacks.

4.2 Phase 2: Execute Attacks

The deduction process is aided by an algorithm that helps to choose and rank the possible attacks based on the information gathering findings.

4.2.1 Attacking Scenario List

Based on the information found in the previous step, different social engineering attacks are possible. To assist the auditor while figuring out which attacks the organization under test is likely to be faced with, a knowledge base was developed. Thus, it is easy to choose attack scenarios that are connected with corresponding information gathering items. These attack scenarios were developed by the help of occurred and public known social engineering incidents, e.g. [11], [8], [4], [2] and derived from the knowledge of other authors e.g. [7] or (Nohlberg, 2008). For a more detailed insight into that list of scenarios please contact the authors. Within these proposed scenarios the security compliance of employees is evaluated by conducting small parts of attacks instead of full attacks (i.e. by establishing a relationship with an employee, without exploiting them). That way, many more different attack vectors can be examined than if just one or two sophisticated and fully exploited attacks were conducted. An example is the Event Registration scenario: Within a spoofed e-mail, the auditor impersonates an employee and pretends to organize a social event. All employees that are interested and would like to get further information should register themselves via an online form. This information could be easily further exploited, but this is not necessary, since we already got a meaningful result.

4.2.2 Usage of the Attacking Scenario List

To choose the *best* attacking scenario we provide the auditors with an algorithm, which will be described later on. It is inevitable that different attacks address different victims, because each attack might increase the employees' suspiciousness towards the social engineering attempts. Clearly, this depends critically on the size of the organization under test. Within a large company, there is no problem to address different employees while in smaller companies only few employees are available as targets for different attacks. Nevertheless, these hindered test conditions form a realistic security estimation for smaller companies, since they are also more resistant to multiple attacks in reality.

To introduce an algorithm for the choice of attacking scenarios, we have to classify them. Therefore, we assign them to different levels of detectability and risk, since these express the main classification quality. The levels of detectability are defined with respect to the sophistication of the attack. Obviously, these levels may vary even within a single scenario, since they critically depend on the actual arrangement of the scenario. For example, a phishing mail can be sent from a freemail address, or from a real company email address that has been spoofed. Moreover, the text can be written in English, or in the company language, it can contain writing errors or be well verbalized. Accordingly, the levels of consequences and risks of a scenario are assigned according to the following scheme:

- Level 1: Helps to gather further non-critical information (e.g. vacation times)
- Level 2: Places malicious file on personal computer via internet or helps to gather further non-critical information (unlimited, i.e. within conversation).
- Level 3: Helps to gather further critical information (i.e. passwords) or places malicious files on personal computer via non secure (physical) way.

- Level 4: Allows physical on-site access to information systems

Well prepared phishing mails mean a huge threat, since they are very efficient and low effort attacking tools. Thus, we further distinguish between different kinds of phishing mails at each level, to cover a broad area of attacks. Therefore, exploitation and preparation mails are sent. The main aim of exploitation mails is to infect the victim's computer with a malicious file. Thus, within an exploitation mail the auditor counts how many people would download a file (i.e. PDF). However, the main aim of a preparation mail is to persuade the victim to enter personal information (i.e. e-mail, name, and password) into a web form. Therefore, the auditor guides the victims to a manipulated website where they shall enter their data.

Since it may not be possible to conduct all tests that are proposed, due to a rising detection risk with each test, the selection of tests is very important. Therefore, the auditor first needs to have conducted information gathering (Process visualized in Figure 2a) and a specification and ordering of the attack scenarios by the following properties: available information (the more the better), risk level (the higher the better) and detectability level. We have developed an algorithm for this process; a diagram can be seen in Figure 2b.

To get an effective insight without immense costs, we recommend conducting attacks beginning with the lowest level of detectability, until one level of attack was successful. An attack can be hold as successful if at least 10 to 30 per cent of victims fall for it (empirical value has to be confirmed in further research). That way, it is possible to make a statement concerning the security of the organization under test. It is recommended to send at least one preparation and one exploitation mail per level, but at best also physical on-site and phone scenarios should be conducted. As a matter of course, the attacks with a higher risk level (within the same level of detectability) are more relevant and should be conducted with priority.

The algorithm for choosing these attacks is as follows: The auditor has to define a priori how many attacks she would like to conduct per level (minimum is two, as there needs to be at least one preparation and one exploitation mail). Then, found information is entered. Based on these findings our algorithm evaluates which attacks got the most information and should be conducted in a more sophisticated way. Within this ordered list, the assigned risk value is not considered. Therefore, the algorithm does two bubble sort iterations where values with a higher risk level are preferred. Based on the resulting list, attacking proposals for the different kinds of attacks can be given. Thus, the algorithm's final output proposes a list of different exploitation/preparation/physical attacking scenarios for each level. Thereby, there are always two to four more scenarios proposed than the auditor has specified a priori. This leaves some freedom in choice of attacking scenarios since an algorithm cannot estimate the whole situation as the auditor can do.

In the following, we describe some of the attack scenarios listed in our knowledge base. We start with an exploitation attack: New Documents (Detectability: 1, 2; Risk: 2) - The auditor pretends to introduce new security documents that should be noticed by all employees working at Computer-Workstations since "there are very important changes". Thus, she attaches a (manipulated) PDF file that gives her access to the opener`s computer. Information that helps at this scenario is i.e. email naming convention, a public forum or IT support handling. But furthermore, we also propose some preparation scenarios, e.g.: Event Registration (Detectability: 1, 2; Risk: 3) -

Within a spoofed mail, the auditor impersonates an employee and pretends to want to organize a social event. All employees that are interested and would like to get further information should register themselves via an online form. The auditor can easily ask for information like name, address, hobbies, e-mails or even passwords. Therefore, it is necessary to know whether there are any websites that are blocked and if there is an intranet in use. In addition, we propose some physical scenarios, e.g.: Repairman (Detectability: 2, 3; Risk: 4) - A hired actor impersonates a computer technician and claims to have the order to service the computer of an employee. While she is doing this, she is snooping around for passwords hidden under the phone, keyboard or desk blotter etc. or plugs an USB-Stick in. Here, it would be beneficial to know if there are public terminals for open use, how the IT support is handled and if there is a public forum where e.g. announcements are made.

At least one employee should be informed as an insider before each executed attack. She should be able to inform the auditor if some internal process goes wrong or prevents the respective attack. Naturally, an IT-Department employee is best suited to collect and report this kind of information. Of course, it has to be ensured that systemic problems discovered in penetration tests are fully tracked and reported well in the resulting document.

Proposed lists, information gathering and penetration testing, can of course be extended following the concept of this paper (necessary to hold the algorithms feasible). Nevertheless, the information gathering list should be adequate for most organizations.

The result of the external testing phase gives an overview of possible attacking vectors for external attackers. We try to pattern how an attacker would approach an attack and to identify which gateways are easy to obey. Since this only gives an overview of apparent attacking gateways, it is necessary to analyze the internal processes as well. It helps to identify even more security issues that arise by reason of internal processes and mistakes.

5 Whitebox Testing

5.1 Phase 1: Analysis of Security Mechanisms Against the Threat of Social Engineering

The internal stage begins with analyzing current security mechanisms. In the literature testing approaches can be found to measure the IT security level of an organization. We derive some key items from [3]. The focus hereby lies on external threats, since the risk that internal attackers (i.e. employees) mean to an organization mostly depends on their satisfaction, not on fails to social engineering. This stage aims to identify vulnerabilities that were overlooked from outside and is supposed to reduce the impact of the residual risk, when the auditor is not capable of conducting adequate attacks.

One part of the process is the reviewing of internal, security relevant documents and policies. Important items that have to be present in order for an organization to be considered as well-protected are listed in our framework. A selection is mentioned here:

- **Rules of Behavior:** A general instruction set for all employees that indicates the desired behavior.
- **Security Mechanisms:** Firewall, USB ports, anti-malware, use of encryption.
- **Termination Responsibilities:** Responsibilities for performing employment termination or change-of employment (including removal of access rights and return of assets)

Furthermore, there are some additional items listed, which are strongly recommended, but not strictly necessary, inter alia a training plan where the frequency and content of training sessions is defined.

Additional documents can affect the assessment in a positive way. Accessibility, availability and update process of all documents has to be reviewed as well.

5.2 Phase 2: Conduct Interviews

Nevertheless, a pure screening of documents cannot tell everything about the real situation within the organization. The spreading process and range is just as important as the content is. To verify this, we propose to do further a check with respect to how well these documents are communicated. Therefore, at least two employees at each level of hierarchy should be additionally interviewed, since that way the risk that both are outlier is minimized. Nevertheless, the possibility of desirability biased results should be taken into account as well. In order to conduct them consistently we have developed an interview guideline, which should be followed while conducting the interviews[1].

Some major items that are covered are as follows:

- Does the employee know any security relevant documents and follows them
- Does the employee write down his/her passwords and keeps them secret
- Would the employee use any USB Sticks without knowing the origin

6 Report

After analyzing the results of this investigation, the organization receives a written report illustrating the results. For the blackbox as well as for the whitebox tests, a rating between zero and 100% is assigned. Since they can be weighted individually, the *weighted average value* can set a meaningful statement, i.e. by assigning more importance to a penetration test phase, which needs more effort and has more significance.

We advise to include a traffic light figure in a prominent place that shows a green, yellow or a red light in order to clearly illustrate this value. Yet, to propose exact values to calculate, evaluate and rank the results more research is necessary.

[1]It is necessary that standards of qualitative interviewing are followed, as they are proposed in [FU07].

7 Conclusion

We have presented a new systematic testing approach for organizations that attaches importance to the threat of social engineering in business contexts. The first part is an external analysis, including an information gathering process and social engineering penetration tests. The second part is an internal investigation that is comprised of an analysis of current security mechanisms and by interviews for a deeper view into the inner workings of the organization under test.

In the external stage the auditor conducts a blackbox penetration test. By help of a knowledge base, she initially gathers information and chooses - based on these findings - attacks out of a list of proposed attacking scenarios. This deduction process is aided by an algorithm that helps to choose and rank the possible attacks based on the information gathering findings in a consistent and systematic manner. Hence, it is necessary that the previously executed information gathering phase is completed beforehand. Nevertheless, it is possible to conduct the external and the internal phase simultaneously while auditors should not be the same person, since – even unintentionally – an auditor could use internal information for his attacking scenarios within e.g. a phone call. In the internal stage the auditor reviews current security mechanisms of the organization under test and confirms the results of this analysis by interviewing employees.

The main drawbacks of this approach are that there is much freedom leftover for the auditor. On the one hand, that way he is able to consider company specific facts, but on the other hand, the test result depends on the ability and creativity of the auditor. We try to decrease this by giving a lot of checklists, but this defect will never disappear. Moreover, there are some design decisions where we had to estimate values to the best of our knowledge (they will be evaluated in a following case study).

The next steps are, of course, a practical evaluation of this concept, where we obtain concrete limits for the different values, gain an insight on problems that still may occur and identify additional social engineering gateways to further improve the accurateness of our social engineering test framework.

References

1. Bowen, P., Hash, J. and Wilson, M. 2006. SP - 800-100.
2. Bright, P. 2014. Anonymous speaks: the inside story of the HBGary hack. [online] Feb 16 2011. Available at: http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/ [Accessed: 27 Mar 2014].
3. Chowanetz, M., Laude, U. and Klinner, K. 2013. "Ein Kennzahlensystem für die Informationssicherheit", paper presented at, 13. Deutscher IT Sicherheitskongress 2013, Bonn, Mai. Bonn: pp. 455-469.
4. Dvorsky, G. 2013. Stuxnet has infected a Russian nuclear plant and the space station. [online] 11. November. Available at: http://io9.com/stuxnet-has-infected-a-russian-nuclear-plant-and-the-sp-1462375259 [Accessed: 27 Mar 2014].
5. Federal Office for Information Security (BSI). 2014. Study - A Penetration Testing Model. BDO, Ernest & Young.
6. Flick, U. 1998. An introduction to qualitative research. London: Sage.
7. Hadnagy, C. 2011. Social engineering. Indianapolis, IN: Wiley.

8. Hadnagy, C. n.d. The Official Social Engineering Framework - Real World Social Engineering Examples. [online] Available at: http://www.social-engineer.org/framework/Real_World_Social_ Engineering_Examples [Accessed: 27 Mar 2014].
9. Hasle, H., Kristiansen, Y., Kintel, K. and Snekkenes, E. 2005. Measuring resistance to social engineering. Springer, pp. 132-143.
10. Herzog, P. 2009. ISECOM - Open Source Security Testing Methodology Manual (OSSTMM). [online] Available at: http://www.isecom.org/osstmm [Accessed: 27 Mar 2014].
11. Holz, T. and Bos, H. 2011. Detection of intrusions and malware, and vulnerability assessment. Berlin: Springer.
12. Nohlberg, M. 2008. Understanding, Measuring and Protecting against Social Engineering Attacks. Ph.D. Stockholm University.
13. Pierce, J., Warren, Matthew and Corray, X. 2004. "A critical review of penetration testing methodologies", paper presented at 5th Australian Information Warfare and Security Conference 2004, Edith Cowan University, Perth, pp. 167-173.
14. Sasse, M. A., Brostoff, S. and Weirich, D. 2001. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. BT technology journal, 19 (3), pp. 122-131.
15. Smith, J. K. and Shorter, J. 2010. Penetration testing: A vital component of an information security strategy. Issues in Information Systems, XI, 1 pp. 358-363.