

# Advanced security methodologies - Penetration testing

M2SSIC-Metz

Pascal Steichen

# Contents

<b>1 Hacking for money</b>	<b>3</b>
1.1 Motivations . . . . .	3
1.2 Limitations . . . . .	4
<b>2 IS and pentesting</b>	<b>5</b>
2.1 Classification (taxonomy) . . . . .	7
2.2 Contract . . . . .	7
2.3 Obligations . . . . .	8
2.4 Requirements . . . . .	10
2.5 Skills . . . . .	13
2.6 Techniques . . . . .	14
2.7 Ethical issues . . . . .	18
2.8 Report . . . . .	20
<b>3 Usual suspects</b>	<b>20</b>
<b>4 Bibliographic references</b>	<b>21</b>

# 1 Hacking for money

Penetration testing, simply put, is finding system vulnerabilities through simulating real-world attack scenario -> "hacking for money"

- **Goals:** Try to find how far a real attacker would make it.
- **Tools:** Well the same as the bad guys: nmap, metasploit, dsniiff ...
- **Method:**
  - contract with "victim"
  - hack, but don't break anything
  - keep confidential information confidential
  - write a detailed report

## 1.1 Motivations

Finding vulnerabilities is an essential step in information security, but the reasons to perform a pentest can be multiple:

- Evaluation of own security concepts

As the biggest enemies of a good security policy are time and money, it is often difficult to have a complete and robust information security concept, that holds of all different attackers.
- To convince management (for budget)

The system administrators often have to balance the features with the security of the internal applications and systems. A pentest done by external experts can therefore help in convincing the management to free budget for vulnerabilities to be fixed.
- To bypass "corporate blindness"

Systems may seem secure from the inside view, but an outsider might have a whole different view of it. Never underestimate the creativeness of a potential intruder.
- Fear of industry espionage, real attacks, etc.

It is always a good thing to test worst-case scenarios, **before** they take place. A denial-of-service for instance is relatively hard to foresee and test internally, so pentests are almost the only solution for these issues.

- Compliance with legal framework

More and more do organisations have to comply to legal obligations, regulations, conventions, standards, etc. only to mention some: cyber-crime convention/framework, data protection laws, SOX, ISO standards, etc.

- Get independent advice

Pentests are normally done by independent experts, which may or may not have more or less information about the "victim" organisation. This independence is important to get a real objective view of its information security.

- Image gain

Well pentest help improve the security and security can be used as **marketing tool**, depending on the sector of course, but at least it can give clients a better confidence in products and services.

## 1.2 Limitations

- It's a "photographer's" approach

As the techniques used by potential attackers rapidly become more sophisticated and new weak points in current applications and IT systems are reported almost daily, one single penetration test cannot yield an assertion about the level of security of the tested systems that will be valid for the future. In extreme cases, a new security loophole may mean that a successful attack could take place immediately after a penetration test has been completed.

- No guarantee that a successful attack will not occur

This in no way means that penetration tests are useless. Thorough penetration testing is no guarantee that a successful attack will not occur, but it does substantially reduce the probability of a successful attack. Because of the rapid pace of developments in IT, the effect of a penetration test is, however, relatively short-lived. The more protection the systems require, the more often penetration testing should be done in order to reduce the probability of a successful attack to a level that is acceptable for the company.

- It does not replace the general security policy nor the usual IT security tests (remember: security is a process)

A penetration test cannot replace the usual IT security tests, nor is it a substitute for a general security policy, etc. An authorization or data backup concept, for instance, can only be tested effectively and

efficiently in other ways. A penetration test supplements established review procedures and tackles the new threats.

## 2 IS and pentesting

Penetration testing can be performed whether the tester has zero, some or total knowledge of the "victim" system. Generally one talks about 2 types of tests:

- Blackbox

A *blackbox* or *zero-knowledge* test is a pentest where the testers have little or no prior knowledge about the target. They have to research the necessary information in publicly available databases or make inquiries as an outsider or anonymous attacker would also have to. The idea behind is of course to determine how much information a potential attacker could get about the "victim's" system and network architecture.

- Whitebox

Here the testers get some knowledge about internal systems and networks or even detailed knowledge about certain areas. It can even go as far as to start with accounts on some systems, like for instance an employee would have. Further types of information, like the internal organisational structure, useful services, like DNS, mail, etc. and maybe some internal procedures are made available to the testers in this type of *whitebox* or *full-knowledge* pentesting.

In general one starts with a blackbox test. If the perimeter security stands tight and no intrusion was possible, it is still necessary to perform a further test: a whitebox. This is because, most systems/networks (~90%) follow the saying: "a crunchy shell around a soft, chewy centre". A whitebox pentest, where for instance, an attack of an employee from the inside, can be simulated, brings up internal holes and security breaches.

The methods of pentesting can vary depending on the way the target systems are being attacked:

- Network-based attacks

"Network-based attacks" are attacks on network components, computer systems and/or applications using network protocol functionalities. This kind of attack exploits vulnerabilities or inadequacies

in hardware and software in order to prepare or carry out attacks. Network-based attacks include port scanning, IP spoofing, sniffing, session hijacking, DoS attacks, buffer overflow and format string attacks, as well as all other exploitation of vulnerabilities in operating systems, application systems and network protocols.

- wireless/mobile (WiFi, bluetooth, Iphone, blackberry...)

More and more organisations use wireless and/or mobile capabilities to enhance the mobility of their employees and the ease of use for clients and visitors, but few of the same companies do consider the fact that this opens a big hole in their network and breaks the perimeter security. As such there can be specific demands for pentesting in these vicinities of the "victim".

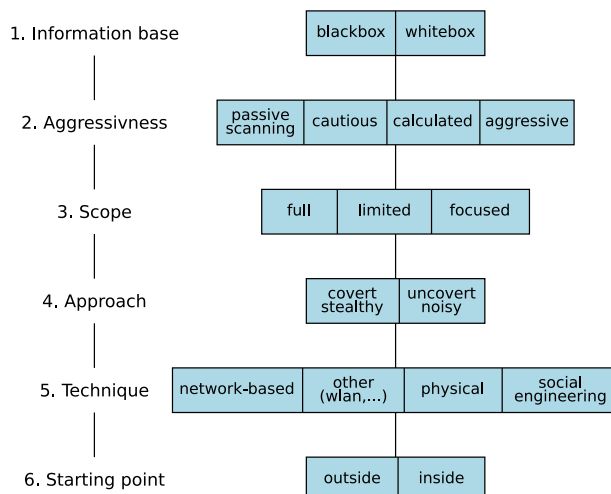
- Social engineering

Social engineering attacks are attempts to manipulate people with privileged knowledge to make them reveal security-related information such as passwords to the attacker. For instance, an attacker could pretend to be an IT employee of an organization and trick an unsuspecting user into revealing his network password. The range of possible attack scenarios is particularly wide with this technique. In its broadest sense, social engineering can also cover situations in which security-related information is obtained by extortion.

- Circumvention of physical security measures

There can be no IT security without the physical security of the technical infrastructure. If physical security measures can be defeated and physical access to IT systems gained, it is usually only a matter of time before an attack on or manipulation of stored applications and data can take place. An example is the unauthorized entry into the computer centre of an organization and the removal of a hard disk on which confidential data are stored. This category also includes the searching of waste for documents with sensitive security-related information (dumpster diving).

## 2.1 Classification (taxonomy)



## 2.2 Contract

- Objective(s) of the penetration test

The contract should clearly state the objective being pursued by the organization commissioning the performance of a penetration test. The most common objectives relevant here are:

- Increasing the security of the technical systems,
- Identifying vulnerability as a criterion for making decisions (e.g. for investments or the suitability of products),
- Obtaining certification/confirmation from an external third party,
- Increasing the security of the organizational/personnel infrastructure.

- Nature of the penetration test

(cf. "Taxonomy" figure)

- Techniques to be used and excluded

The individual techniques used in a penetration test are to be described in more detail where this is both possible and appropriate. In particular, any social engineering techniques and active tests of access controls to be employed should be described. Because social engineering techniques are by nature problematic and possibly unethical, it is

appropriate to specify a clear framework for them (e.g. avoiding incitement of employees to behave unethically). An active test of access controls attempts to circumvent physical security measures, which can be regarded as burglary. An explanation of the circumstances under which the test is to take place is also necessary in this respect.

It is also important to exclude attacking techniques which are expressly not to be used. Such techniques should also be defined in the contract, stating the reasons for their exclusion.

- Joker

The *joker* is a special contractual agreement, where the testers get a kind of "own this service or system" card at certain moments during the overall pentest. In this way services or systems which were not penetrated or exploited, can however be considered to be so and as such 0days or alike can be more easily tested. Special fall-back or worst-case scenarios can be tested this way as well as "defence in depth" mechanisms, without wasting valuable time.

## 2.3 Obligations

- The Client

- Provision of information depending on the nature of the penetration test

Depending on the nature of the penetration test, the penetration tester may be reliant on extensive information from the client. For example, a white-box test requires information on DNS names, IP addresses, security policies, system configurations, firewall rules, escalation procedures, etc. The penetration tester should therefore provide the client with a list of the required information before concluding the contract and agree in the contract that all required information be made available in time.

- Information from potentially affected third persons

During normal data traffic on public networks, a penetration test also uses third party systems (e.g. the communication server of a provider, the web server of a mainframe computer). Since it is impossible to exclude impairing the performance of these systems, we advise giving advance notification of the penetration tests to any third persons who may be affected. These information duties could be delegated to the client as it is in a better position to estimate which third parties could be affected by the tests.

- Protective measures for unforeseeable system failure

Since it cannot be completely ruled out that systems are impaired during testing such that data is lost, it is in the client's own interests to create data backups of the high-risk and relevant systems. Data backups ensure that the data can be recovered if necessary and mitigate the potentially adverse effects of data loss.

- The Testers

- Secrecy

In the course of a penetration test, a penetration tester may gain access to highly sensitive information on vulnerabilities in the client's network. This information must not be made available to third persons so as to reduce the risk to the client to a minimum. The tester should therefore be bound to observe secrecy in respect of the information made available to him as well as the information which came to his knowledge in the course of testing. Generally an NDA (Non Disclosure Agreement) is signed with the client.

- Compliance with licensing regulations

The tester is responsible for complying with licensing regulations when using commercial security tools. Since the royalties for the use of security tools are normally charged on to the client, the client should be provided with a clear breakdown of these charges.

- Documenting the testing procedures and results

The nature and scope of the documentation of the testing procedures and the results should be specified in the contract. The tester should be obliged to provide precise documentation of his testing procedures. This ensures that the techniques he has used can be traced in the event of damage. In addition, the parties should agree to the form in which the results should be presented (report, presentation, reports and analyses of the security tools used).

- General duty of due care

The penetration tester must exercise due care while performing testing procedures. For example, it would be grossly negligent if the penetration tester were to "accidentally" attack the system of an uninvolved third party because he had confused a DNS name. The contract should therefore stipulate that the penetration tester must apply due care in the performance of his activity with respect to potential damage he may cause.

## 2.4 Requirements

The following organizational requirements should be clarified with the client in the run-up to a planned penetration test.

- Who, apart from the client, will be affected either directly or indirectly by the penetration test?

In addition to the client's system, the systems of the provider, which may even be physically located on the client's premises while being administered by the provider, are often affected by the penetration test. In order to avoid misunderstandings, the provider should therefore be notified of the planned penetration test. Some testing steps, e.g. DoS tests, can, due to their high bandwidth requirements or non-standard data packages, also lead to disruptions to providers' network components and should therefore be discussed in detail beforehand with the providers. If certain functions have been outsourced (e.g. webhosting the WWW server), the systems involved should be excluded from the penetration test. If these systems are included in the penetration test, written approval must for this be sought from the system operator or outsourcing operator.

The tester must note that he is responsible for the security of IT systems, including outsourced systems, e.g. for the integrity of the accounting data, and that this responsibility cannot be simply transferred to the outsourcing service provider.

- Have the liability risks received appropriate consideration?

The penetration tester should have liability insurance with sufficient cover to insure himself against possible claims for damages of third parties. Although care should be taken to minimize potential risks for third party systems before testing, disruptions to third party systems cannot be completely ruled out.

- What needs to be considered in respect of the time of testing?

Penetration tests can impair the functionality of production systems. Since the aim of a test is to detect vulnerabilities, but without endangering orderly operations, the actual attacks should take place at a time agreed to by both parties. This should be considered in the planning stage in the run-up to the penetration tests. Penetration tests often take place in a period of several days. Times should be chosen at which neither crucial processing is performed nor high volumes of on-line orders, for instance, are processed on the target system. Consideration can be shown for the time at which the attacks are carried out in white-box tests only. With black-box approaches, information

on the level of criticality and system utilization at certain times is not normally available.

- What needs be done in the event of system failure or other emergency?

In case the system fails despite care being exercised during testing, or in case of another emergency, e.g. a serious disruption of the system, contingency measures will need to be defined. The contract must at least specify who to notify and when in case of a suspected or identified failure or disruption. In addition, the kinds of faults that have to be reported should be defined. The following "disruptions" can be distinguished:

- Complete system failure
- Partial failure of certain subsystems
- Incorrect responses from the system
- Large increase in the length of the system's response times
- Countermeasures being taken in response to a covert penetration test
- Attacks of third parties on the system

- Which of the client's employees are affected by the penetration test?

The number of employees affected by testing will depend on the scope and nature of the test. A penetration test limited to a test system will only be able to affect the administrators and the users of the test system. As well as the system users, a test which also examines production systems can, in extreme cases, also affect all employees who are in some way reliant on the results of the systems being tested, or hinder them in their work. If social engineering techniques are to be used in the penetration test, the parties should agree on the employees who may be targeted during testing and the extent to which this is permissible.

- How much time and cost will the penetration test involve for the client?

The client must expect possible impairment to his IT systems as a result of the penetration test which may result in irregularities in operations. It is therefore necessary to take steps before a penetration test in order to keep the effects of potential disruptions to a minimum. These may include, for example, assigning an employee to monitor the penetration test from the client's perspective and who can halt testing if necessary. The client should also consider making (additional) backups before a penetration test is performed. It is also necessary to adopt an contingency plan (if there is not one already) and escalation

procedures which facilitate both an orderly course of action and the introduction of suitable countermeasures. If the white-box approach is chosen for the penetration test, additional information and professional contact partners must be made available to the penetration tester.

- How much time and effort will the penetration test require of the tester?

In order to be able to assess whether a service provider can adequately perform a penetration test and if so, the approximate expense that this would involve, the time and effort required of the tester to perform the penetration test must first be quantified. The following aspects should be considered:

- Objective and scope of the penetration test

The tester and the client jointly define the nature of the penetration test and the test procedures to be performed in line with the objective of the penetration test. Depending on the nature and scope of the penetration tests, it may be possible to determine the resources the penetration tester will need to use (hardware, software, suitable employees) before the actual start of testing.

- The size of the infrastructure to be tested

The size of the infrastructure is often expressed in the number of IP addresses that are to be tested. Generally, it is not possible to specify the time a tester will need to spend on the penetration testing of an individual system since this depends on the model and the configuration of the system, the experience and dedication of the tester as well as on other factors. Another factor is whether the system to be tested is located in a logical segment whose gateway to a public network is protected by a central firewall, or whether it is a divided infrastructure with several different gateways to public networks. As these factors are difficult to quantify, we can only derive the very general statement that the greater the number of systems and the larger the infrastructures to be tested, the more time and effort is required of the tester.

- The complexity of the infrastructure to be tested

The complexity of the infrastructure to be tested is a further important factor that influences the time and effort the penetration tester has to expend. Typical services that are offered on the internet are the retrieval of websites (HTTP), downloads (FTP) and e-mail communication. Vulnerabilities in applications that support these services are often known as such services are very common; they are published at many places on the internet. If a company or public authority limits itself to such widespread

services, an infrastructure with a low level of complexity can be assumed. The amount of time and manpower involved in performing a penetration test should therefore be relatively small. If complex e-commerce solutions or interactive applications are used in addition, it will take longer to locate vulnerabilities and a higher degree of expertise may be needed to exploit them. This means that the penetration tester will need to allow for a longer period of time and more experienced personnel for performing the penetration test.

## 2.5 Skills

The following skills are necessary for an expert performance of penetration tests:

- Knowledge of system administration/operating systems  
This knowledge is necessary for evaluating weaknesses in the operating systems of the target systems and also facilitates the handling of the systems used in the penetration test.
- Knowledge of TCP/IP and, if applicable, other network protocols  
Since data traffic on the internet is handled by TCP/IP, which has also become the standard in LANs, in-depth knowledge of this protocol is essential. Knowledge of TCP/IP is closely connected with knowledge of other networks and of the OSI reference model.
- Knowledge of programming languages  
To be in a position to exploit vulnerabilities in applications and systems, knowledge of a programming language is advantageous. While there are a range of ready tools as scripts or with graphical user interfaces, security gaps such as buffer overflows etc. can only be effectively exploited when the tester has the necessary programming knowledge.
- Knowledge of IT security products such as firewalls, intrusion detection systems  
Since security arrangements such as firewalls or intrusion detection systems are extremely common nowadays, the penetration tester should know how these security arrangements work and follow the latest reports on security gaps in IT security products. It is essential to have an overview of the common products on the market in the field of IT security.

- Knowledge of how to handle hacker tools and vulnerability scanners

In addition to some basic knowledge, experience in handling hacker tools and vulnerability scanners is necessary for performing penetration tests. Skills in the handling of these tools should be obtained through practical experience. Over the course of time, among the multitude of tools available, certain products have achieved a wide distribution (e.g. nmap for port scans, L0phtcrack for Windows passwords). Commercial tools can be used for performing an efficient test and free-ware tools can be employed to demonstrate the relatively simple performance of such tests. The efficiency of the penetration test depends heavily on how experienced the penetration tester is in handling these tools.

- Knowledge of applications/application systems

Many vulnerabilities are located in the applications rather than the operating system software. They span the entire range of application systems, ranging from insufficiently secured macro functions in word processing programs to vulnerabilities of internet browsers through scripting, to buffer overflow errors in large database systems, as examples. The tester should therefore be familiar with as many types of applications as possible. Detailed knowledge of commonly used applications is particularly important, since the risk of hackers and crackers here is generally particularly high.

- Creativity

In addition to the high professional requirements, creativity is an important quality in a penetration tester. Since a qualified penetration test can only follow a rigid pattern to a limited extent, the question of how to proceed at a particular point will undoubtedly arise during the course of a penetration test when it at first sight seems impossible to further compromise a system. This problem can be approached by cleverly combining the information a tester has obtained, the vulnerabilities he has identified and the tools and methods available to him. By exercising his intelligence, a creative penetration tester should therefore be better positioned to perform a "successful" test than a penetration tester who merely relies on the results of his tools when performing the test. Creativity should, however, never lead to an un-systematic or even chaotic test which is not subsequently traceable.

## 2.6 Techniques

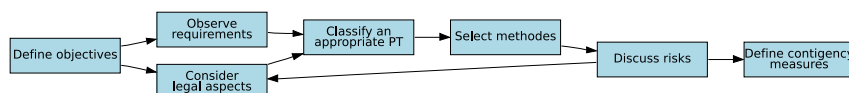
Penetration testing must be done in a structured manner using well-defined steps:

1. Preparation
  2. Reconnaissance
  3. Enumeration
  4. Exploitation
  5. Reporting
- Documentation (throughout the process)

## 1. Preparation

At the start of a penetration test the client's objectives must be clarified with him and defined. The performance of a penetration test without taking full account of the relevant legal provisions could have consequences under criminal or civil law. The tester must therefore ensure that the test procedures are not going to infringe legal provisions or contractual agreements. The failure of a production system could also lead to recourse demands as a result of penetration techniques which have not been agreed to or risks associated with the techniques used that were not made known, which is why the procedure and its risks must be discussed and documented.

All details agreed to should be put in writing in the contract.



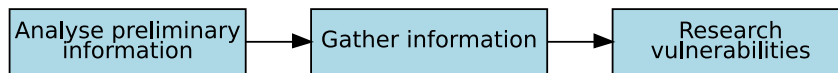
## 2. Reconnaissance

This phase is the passive penetration test.

The aim is to obtain a complete and detailed overview of the systems installed, including areas open to attack or known security shortcomings. Depending on the number of computers or the size of the network to be examined, the test steps may be extremely time-consuming. If, for example, a class C network (256 possible IP addresses) behind a firewall has to be fully tested, a full port scan (all 65536 ports) may take several weeks depending on the setting. While these long test steps are usually performed automatically, the time required for them still needs to be taken into account in the

planning. Thus a penetration test can take 20 days, for example, with the aforementioned test lasting several weeks.

Freely accessible databases can provide much information about an organization.



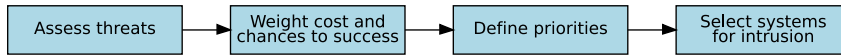
### 3. Enumeration (analysing information and risks)

A successful, transparent and economically efficient procedure must analyse and assess the information gathered before the test steps for actively penetrating the system - which are often extremely time-consuming - can be performed. The analysis must include the defined goals of the penetration test, the potential risks to the system and the estimated time required for evaluating the potential security flaws for the subsequent active penetration attempts. The targets for exploitation are then selected on the basis of this analysis. From the list of identified systems the tester may, for example, choose to test only those which contain known potential vulnerabilities due to their configuration or the identified applications/services or those about which the tester is particularly knowledgeable.

The selection must be comprehensively documented and justified since in addition to the desired improvement in efficiency, they also lead to a reduction in the informative value of the penetration test and the client needs to be made aware of this.

Steps are as follows:

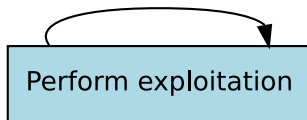
- Scan target systems for services.  
An attempt is made to conduct a port scan of the computer(s) being tested, open ports being indicative of the applications assigned to them.
- Identify systems and applications.  
The names and version of operating systems and applications in the target systems can be identified by "fingerprinting".
- Researching Vulnerabilities.  
Information about vulnerabilities of specific operating systems and applications can be researched efficiently using the information gathered.



#### 4. Exploitation (active intrusion attempts)

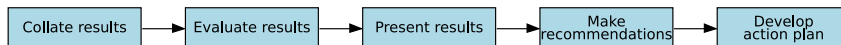
Finally, the selected systems are actively assailed. This phase entails the highest risk within a penetration test and should be performed with due care. However, only this phase reveals the extent to which the supposed vulnerabilities identified in the reconnaissance phase present actual risks. This phase must be performed if a verification of potential vulnerabilities is required. For systems with very high availability or integrity requirements, the potential effects need to be carefully considered before performing critical test procedures, such as the utilization of buffer overflow exploits. Exploited vulnerabilities can be used to obtain unauthorized access to the system or to prepare further attacks.

In a white-box test, a patch may need to be installed on critical systems before performing the test to prevent system failure. The test will probably not be able to locate any vulnerabilities, but will document the security of the system. Unlike a hacking attack, however, the penetration test is not complete - it has to be continued.



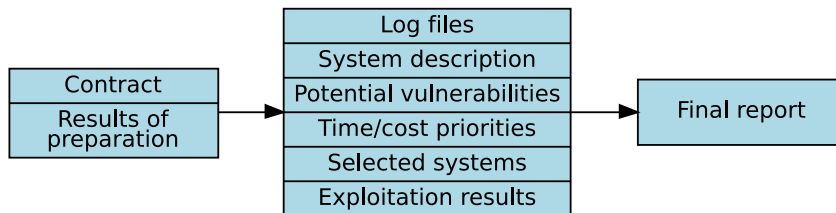
#### 5. Reporting (final analysis)

This is the less fun part, but by far the most important for the target. The report should contain an evaluation of the vulnerabilities located in the form of potential risks and recommendations for eliminating the vulnerabilities and risks. The report must guarantee the transparency of the tests and the vulnerabilities it disclosed. The findings and resultant risks for IT security should be discussed in detail with the client after the conclusion of the test procedures.



#### Documentation

The penetration test documentation should be compiled during phases 1 to 5 and not just as part of the final analysis in phase 5. This ensures that the test steps and results of all phases are documented and makes the penetration test transparent and traceable.



## 2.7 Ethical issues

There are a number of **ethical issues** that need to be considered before starting penetration testing.

- Usage of *social engineering* techniques should be clarified and justified.
- *Exploitation of vulnerabilities* (to what extent) should be discussed.
- A penetration test is ever only a commissioned activity (any proactive behaviour is unacceptable, i.e. launching an attack attempt without a mandate should always be considered a punishable attack).

- **Social engineering**

These techniques work because all human beings possess certain characteristics or weaknesses that can be exploited. These include positive characteristics such as

- the tendency to be amiable,
- have a feeling of moral obligation and be helpful,

as well as less positive qualities such as being

- opportunistic
- and unwilling to assume responsibility.

Almost all employees would, for example, provide the "new boss" with confidential information at his/her request if he or she acts self-confidently and appears genuine. People do this out of a willingness

to help on the one hand, and out of a sense of duty, but also, on the other hand, as a result of opportunistic considerations. These kinds of weaknesses can only be counteracted by providing all employees with regular training.

One could, however, also contend that social engineering techniques are successful because of insufficient or inappropriate security measures. If, for example, passwords are issued automatically and are so complicated that they are almost impossible to memorize, many users will make a note of them in "safe" places. Or they often forget their passwords and request new passwords, which is also a good starting point for social engineering.

Since the use of social engineering techniques has a direct influence on the client's employees in that they assess their reliability or security awareness, they could make those involved apprehensive. This could be all the more so when social engineering techniques are performed without prior warning and are subsequently explained. Even when the penetration test result report does not include any information or names, and no personal information on the improper conduct of certain employees is transmitted orally to the client, these techniques can still make employees feel insecure.

These are the reasons why many security experts reject the use of social engineering in security tests or only deem them appropriate when security requirements are very high. The use of social engineering therefore needs to be considered very carefully. The tester should always inform the client of the possible consequences of social engineering and state that this technique will most probably succeed if users are given no prior training and that this could have adverse affects on employees.

- **Vulnerabilities exploitation**

A vulnerability in an application or an operating system which can then be exploited to take over a system will normally be identified before the system is actually compromised. Here, the tester should consider whether this last step of exploiting the vulnerability needs to be carried out in order to verify it, or whether it is sufficient to merely point out the existence of the vulnerability.

This question can only be resolved by keeping in mind the defined objective of the test and the conditions derived from this. If the penetration test is to be as realistic and informative as possible, it may be appropriate not to impose any limits on the aggressiveness of testing procedures. If, on the other hand, a potential disruption to operations is to be avoided as far as possible, vulnerabilities should not be actively exploited. In this case, the result of the penetration test would be the

identification of existing vulnerabilities and no evidence of a successful penetration would be provided.

## 2.8 Report

The report should contain the following elements:

- Management summary

A short and precise summary showing the main issues detected and giving a global picture on the current security situation of the organisation.

- Detailed technical analysis

The intended audience of this part are the system administrators and or security officers. It should contain a detailed listing of all the vulnerabilities, intrusion, exploited systems, etc. Every point should include a description of the problem encountered, a risk analysis for this issue and proposals for solutions.

The report itself is of course essential for the client, but there's something more important, that is most often not recognized:

- Meeting

Indeed the report should not simply be given, but discussed in detail during a meeting with all the parties, sysadmins and management. In fact the report is often used as an awareness raising tool for the management or the inexperienced sysadmins.

## 3 Usual suspects

### or where to begin

Similar to a real attack, the pentester uses well known methods and ways for performing their mission:

*Start with the usual suspects, then follow your stomach, there is no cookbook-way.*

- Reconnaissance:

- website and other homepages
  - Google
  - DNS
  - whois / RIPE
- Enumeration:
  - port scanning
  - known vulnerabilities first
  - default or error configs
- Exploitation:
  - old versions
  - weak passwords and/or configs
  - unused or forgotten services
  - client-side software (flash, ...)
  - open shares
  - WLAN
  - backups
  - physical negligence

## 4 Bibliographic references

- [A Penetration Testing Model \(BSI\)](#)
- [OSSTMM](#)
- [Are there perils in penetration testing?](#)
- [RedTeam gmbh](#)