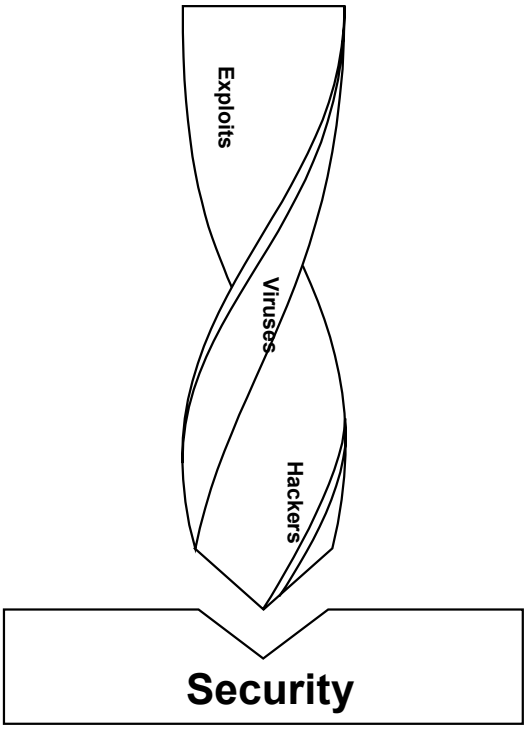
Study

A Penetration Testing Model



Contents

1 Introduction and Objectives of this Study

This study on "A Penetration Testing Model" addresses the use of penetration testing in security-relevant IT systems. The security of systems that are linked to public networks can be compromised by unauthorized, and usually anonymous, attempts to access them. This situation calls for test methods that are devised from the attacker's perspective to ensure that test conditions are as realistic as possible.

Technically speaking, a penetration test is the controlled attempt at penetrating a computer system or network from "outside" in order to detect vulnerabilities. It employs the same or similar techniques to those used in a genuine attack. Appropriate measures can then be taken to eliminate the vulnerabilities before they can be exploited by unauthorized third parties.

This study is aimed at businesses and institutions which offer, or are planning to offer, penetration tests. It presents a structured approach to penetration testing that facilitates - and can ensure - the efficient and focused performance of such tests. The study is also designed to provide assistance with selection criteria to decision-makers in private and public entities who are planning to commission a penetration test.

This study is not a guide to hacking networks and systems, which is why the authors have consciously refrained from including detailed technical instructions and descriptions of the tools used in penetration testing.

1.1 Introduction to Penetration Testing

By using public networks businesses and public authorities are exposed to numerous risks. Public and private entities are often unable to grasp the full extent of today's complex communication structures and frequently have little or no control over them. Enterprises and public authorities connect to the internet, thereby yielding some of their responsibility (e.g. availability of external servers and networks), but also exposing themselves to new threats which need to be tackled appropriately.

1.2 Methodology and Structure of this Study

The structure of this study follows that of the penetration testing process, from a request for a proposal to test completion, including the necessary documentation. As a result, the methodology itself and its application are described at the end of the study. This means that the reader can either be guided through a defined process or go straight to the chapters of interest.

This study does not have to be read in a particular order to be understood, provided that the reader possesses the relevant specialist knowledge.

The first chapter of this study contains a general introduction to the subject of penetration testing. It includes a definition of target groups and a description of the structure of this study. For the interested reader, the second chapter contains a brief introduction to IT security.

The third chapter is an attempt at positioning penetration testing within the testing and auditing system by its goals ("what goals can be achieved with penetration tests?"), definitions ("what distinguishes a penetration test from an audit?"), and classifications ("what criteria should a penetration test fulfill?").

The fourth chapter deals with legal issues, with the focus more on civil law than criminal law aspects.

The underlying conditions and organizational, personnel and technical requirements are addressed in the fifth chapter, with special emphasis on "ethical" issues to highlight the limits of penetration testing and the appropriateness of the means.

Once all the prerequisites for penetration testing have been discussed, the methodology and documentation of such tests are described in detail.

For ease of comprehension, we explain how the method is implemented in the seventh chapter "performance of penetration tests". In keeping with the practical nature of this study, the reader is given instructions on how to follow the individual steps to facilitate their application in public or private entities.

Information that is of interest but not directly related to the subject can be found in the appendix. The reader is provided with details about penetration test certification, further methodological information and suggestions for forms to be used.

2 IT Security and Penetration Testing

Penetration testing can reveal to what extent the security of IT systems is threatened by attacks by hackers, crackers, etc., and whether the security measures in place are currently capable of ensuring IT security. For a clearer picture of the risks to IT security, this chapter begins with a summary of the current threats, describing the most common intruder profiles and widespread techniques for attacking IT systems. This is followed by a brief account of typical IT security measures, some of which can be tested with penetration tests. Finally, the process of devising penetration tests is explained.

2.1 Threats

A joint study by the US Computer Security Institute (CSI) and the FBI [CSI02, p. 11] found that in 2001 the companies questioned had sustained average losses of US$4.5m from information theft as a result of computer crime. Intruders can have a range of motives for carrying out attacks on IT infrastructure. The major intruder groups and their motives are outlined below.

2.1.1 Intruder Profiles

In the media, the term “hacker” is used to refer to any person who intrudes into other IT systems without authorization. However, a finer distinction is often made between “hackers”, “crackers” and “script kiddies”. Whereas “hackers” are regarded as being experimentally-minded programmers who target security loopholes in IT systems for technical reasons, “crackers” are people with criminal energy who exploit weak points of IT systems to gain illegal advantages, social attention or respect.

“Script kiddies” are usually intruders lacking in-depth background knowledge and driven by curiosity who mainly direct attack tools downloaded from the internet against arbitrary or prominent targets.

Crackers possessing privileged knowledge about the organization they are attacking are termed “insiders”. Insiders are often frustrated (former) employees of an organization who use their knowledge of internal affairs to harm that organization. The danger posed by insiders is particularly great because they are familiar with the technical and organizational infrastructure and may already know about existing vulnerabilities.

In addition to the categories described above, industrial espionage also poses a serious threat. The aim of industrial espionage is to gain knowledge of business secrets such as innovative technical designs, strategies and ideas that help in gaining a competitive edge and to use such information for personal benefit.

2.1.2 Methods

There are several ways of manipulating or damaging IT systems and of preparing an attack on IT systems.

- 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.

- 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 center 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).

2.2 IT Security Measures

Measures to improve IT security are needed to combat the threats described above. However, one hundred-percent security can never be attained. Organizational measures, such as IT security organization and escalation rules, and technical measures, such as access controls, encryption and firewalls, are employed to establish a certain level of IT security.

In line with the company IT security policy, all such measures are described in an IT security concept that is valid for the entire organization.

If the organization being tested is unable to present a security concept or security policies, it is doubtful whether penetration testing is meaningful, especially when the IT landscape is complex. In such cases, IT security could probably be improved far more efficiently by first devising and implementing an appropriate security concept.

2.3 Devising Penetration Tests

The term “penetration test” and the methods used for testing were established in 1995 when the first Unix-based vulnerability scanner “SATAN” [Venema95] was introduced. At that time the program was the first tool that was able to automatically scan computers to identify vulnerabilities.

Nowadays, there are a number of freeware and commercial vulnerability scanners, most of which have an updatable database of known hardware and software vulnerabilities. These tools are a convenient way of identifying vulnerabilities in the systems being tested and therefore of determining the risks involved. Ordinarily, the information provided by such tools comprises a technical description of the vulnerability and also gives instructions as to how to eliminate a weak point by altering configuration settings.

In addition, a large number of freeware tools for carrying out or preparing attacks on internet computers and networks can be found on the internet.

2.4 Penetration Testing Procedures

The procedure for penetration testing should follow the steps described below.

1. **Research information about the target system**

   Computers that can be accessed over the internet must have an official IP address. Freely accessible databases provide information about the IP address blocks assigned to an organization.

2. **Scan target systems for services on offer**

   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.

3. **Identify systems and applications**

   The names and version of operating systems and applications in the target systems can be identified by "fingerprinting".

4. **Researching Vulnerabilities**

   Information about vulnerabilities of specific operating systems and applications can be researched efficiently using the information gathered.

5. **Exploiting vulnerabilities**

   Detected vulnerabilities can be used to obtain unauthorized access to the system or to prepare further attacks.

The quality and value of a penetration test depends primarily on the extent to which the test caters to the client's personal situation, i.e. how much of the tester's time and resources are spent on detecting vulnerabilities related to the IT infrastructure and how creative the tester's approach is. This process cannot be covered in the general description above, which is why there are huge differences in the quality of penetration testing as a service.

3 Classification and Objectives of Penetration Testing

This chapter outlines the possible starting points and access channels for a penetration test, the IT security and protection measures that can be tested, and how the tests differ from general IT security reviews and IT audits.

3.1 Starting Points and Access Channels for Penetration Tests

Typical starting points or points of attack for a penetration test are firewalls, web servers, RAS access points (e.g. modems, remote maintenance access points), and wireless networks. Given their function as a gateway between the internet and the company network, firewalls are obvious targets for attack attempts and starting points for penetration tests. Web servers have a high risk potential because of their manifold functions and the resulting vulnerabilities. Other servers that offer services that are accessible externally, such as e-mail, FTP and DNS, should be included in the test, as should "normal" workstations.

3.1.1 Testable IT Security Measures

A penetration test should test both logical IT security measures such as passwords, and physical measures such as access control systems. Frequently only logical controls are tested as this can usually be done remotely via the network which makes the tests less time-consuming, and because the probability of attacks on logical IT controls is thought to be far greater.

3.1.2 Penetration Testing, IT Security Audit, IT Audit

"Crackers" aim to access protected data or maliciously disrupt data processing. Unlike penetration testing, the purpose of security audits and IT audits is to generally examine the IT infrastructure in terms of its compliance, efficiency, effectiveness, etc. They are not necessarily aimed at detecting vulnerable points. For instance, a penetration test does not involve verifying whether in the event of hardware damage certain data could be restored with a regular backup; it only checks whether such data could be accessed. This could also be done in a security audit or an IT audit, but normally from a different perspective and not in the technical depth characteristic of a penetration test.

3.2 Objectives of Penetration Testing

For a successful penetration test that meets the client's expectations, the clear definition of goals is absolutely essential. If goals cannot be attained or cannot be achieved efficiently, the tester should notify the client in the preparation phase and recommend alternative procedures such as an IT audit or IT security consulting services.

Client goals that can be attained by penetration testing can be divided into four categories:

1. Improving security of technical systems
2. Identifying vulnerabilities
3. Having IT security confirmed by an external third party
4. Improving security of organizational and personnel infrastructure

The result of an IT penetration test should therefore be more than just a list of existing vulnerabilities; ideally it should also suggest specific solutions for their elimination.

Below the four goal categories are discussed, with examples.

3.2.1 Improving Security of Technical Systems

Most penetration tests are commissioned with the objective of improving the security of technical systems. The tests are confined to technical systems such as firewalls, routers, web servers, etc., with organizational and personnel infrastructure not being explicitly tested. One example is a penetration test to expressly check whether unauthorized third parties are able to access systems within the company's LAN from the internet. Possible test results or findings are unnecessary open firewall ports or vulnerable versions of internet applications and operating systems.

3.2.2 Identifying Vulnerabilities

In contrast to the other three goals, identification is the actual objective of the test. For example, before combining two LANs in the wake of a company merger, the new LAN can be tested to see whether it is possible to penetrate it from outside. If this can be done in the penetration test, action has to be taken to secure the interface before the merger, or the two networks should not be combined at all.

3.2.3 Having IT Security Confirmed by an External Third Party

A penetration test can also be conducted to obtain confirmation from an independent external third party. It is important to note that a penetration test only ever reflects the situation at a particular point in time and cannot therefore yield assertions about the level of security that are valid in the future.

Nevertheless, regular penetration testing may be suitable for demonstrating the increased security of customer data in a webshop or other internet application.

3.2.4 Improving Security of Organizational and Personnel Infrastructure

Apart from testing the technical infrastructure, a penetration test can also test the organizational and personnel infrastructure, to monitor escalation procedures, for instance, with the scope and/or aggressiveness of the tests being increased step by step. Social engineering techniques, such as requesting passwords over the telephone, can be employed to assess the level of general security awareness and the effectiveness of security policies and user agreements.

The scope of such tests needs to be defined precisely in advance (see also section **5.4 Ethical Issues**).

3.3 Limits of Penetration Testing

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.

However, 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.

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.

3.4 Classification

What criteria can be used to describe a penetration test, or what distinguishes one penetration test from another? Distinguishing features, such as the extent of the systems tested, the cautiousness or aggressiveness of testing, etc., that characterize a specific penetration test have to be adapted to suit the goal of the test to ensure efficient and effective testing with a calculated risk. **Figure 1** shows a classification of possible penetration tests. On the left are six criteria for defining penetration tests, on the right are the various values for the criteria summarized in a compact tree diagram.

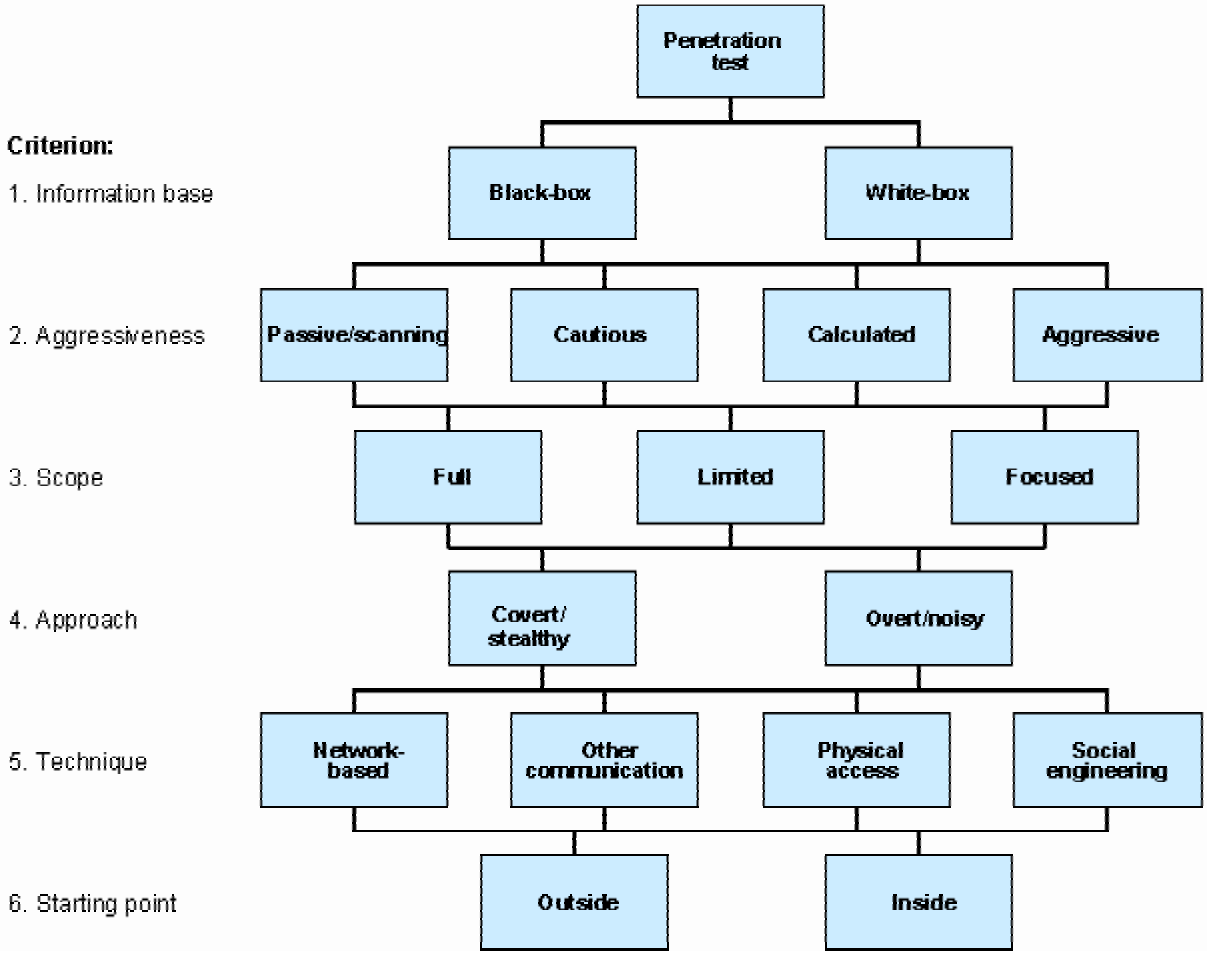


Figure 1: Classification of penetration tests

An appropriate penetration test – to meet the client's goals - has to be defined on the basis of the above criteria. It should be noted that not all possible combinations are useful tests even though the criteria in the classification have been kept as distinct as possible. An aggressive test is usually identified very quickly and is therefore not ideal in combination with stealth techniques. Similarly, an overt penetration test is not suitable, for example, for obtaining confidential information from employees warned in advance by means of social engineering techniques.

The six criteria and their possible values are discussed below:

1. **Information base:** What is the penetration tester's initial level of knowledge about the target network or object?

   A fundamental distinction is made between black-box testing, without any insider knowledge, and white-box testing, where the tester has insider knowledge:

1. A **black-box** test realistically simulates an attack by a typical internet hacker. The hacker has to research the necessary information in publicly available databases or make inquiries as an outsider.

2. In a **white-box** test an attack by a (former) employee or external service provider with detailed knowledge in certain areas. The extent of such knowledge can range from limited, e.g. as possessed by an employee who has worked in the company for only a short time, to in-depth system knowledge, such as that gained by an external IT service provider who has installed security-relevant systems.

2. **Aggressiveness**: How aggressive is the penetration tester during testing?

   To allow a sufficiently fine distinction, four levels of aggressiveness are defined for the purposes of this study:

   - With the lowest level the test objects are investigated **passively** only, i.e. any vulnerabilities that are detected are not exploited.
   - With the second level – **cautious** – identified vulnerabilities are only exploited when, to the best of the tester's knowledge, the system being tested will not suffer as a result, e.g. using known default passwords or trying to access directories on a web server.
   - With the next level – **calculated** – the tester also attempts to exploit vulnerabilities that might result in system disruptions. This includes, for instance, automatically trying out passwords and exploiting known buffer overflows in precisely identified target systems. Before taking such steps, the tester considers how likely they are to be successful and how serious the consequences would be.
   - With the highest level – **aggressive** – the tester tries to exploit all potential vulnerabilities, e.g. buffer overflows are used even on target systems that are not clearly identified, or security systems are deactivated by deliberate overloading (denial of service (DoS)) attacks. The tester has to be aware that, in addition to the systems being tested, neighboring systems or network components might also fail as a result of these tests.

3. **Scope**: Which systems are to be tested?

   When a penetration test is being carried out for the first time, a full test is advisable to ensure that no security loopholes are overlooked in systems that have not been tested.

   The time required for a penetration test is normally directly related to the scope of the systems to be investigated. Identical and near-identical systems can often be investigated in a single test, but as soon as there are different configurations, each system will need to be dealt with separately:

   - If only a specific sub-network, system or service is to be tested, for the purposes of this study the penetration test is termed **focused**. This test scope is appropriate after a modification or extension of the system landscape, for instance. Such a test can, of

course, only provide information about the system that was tested; it cannot provide general information about IT security.

- In a **limited** penetration test, a limited number of systems or services are examined. For example, all systems in the DMZ, or systems comprising a functional unit can be tested.
- A **full** test covers all available systems. It should be noted that even in a complete test certain systems, e.g. outsourced and externally hosted systems, might not be able to be tested (see Section 5.1).

4. **Approach**: How "visible" is the team during testing?

   If, in addition to the primary security systems, secondary systems - such as an IDS, or organizational or personnel structures (e.g. escalation procedures) - are to be tested, the testing approach will have to be adapted accordingly:

   - The penetration tests carried out on secondary security systems and existing escalation procedures should – at least in the beginning – be **covert**, i.e. in the initial survey stage only methods that are not directly identifiable as attempts at attacking the system should be employed.
   - If the covert approach fails to generate a reaction, or a white-box test is carried out in collaboration with those responsible for the system, **overt** methods, such as extensive port scans with a direct connection, may be employed. The client's staff may be included in the team conducting an overt white-box test. This is particularly advisable with highly critical systems because it means that the testers are able to react faster to unexpected problems.

5. **Technique**: What techniques are used for testing?

   In a conventional penetration test, systems are attacked via the network only. In addition, other types of physical attacks and social engineering techniques can be used to attack systems.

   - A **network-based** penetration test is the normal procedure, and simulates a typical hacker attack. Most IT networks currently use the TCP/IP protocol, which is why such tests are also called IP-based penetration tests.
   - Apart from TCP/IP networks there are **other communication networks** that can also be used for staging an attack. These include telephone and fax networks, wireless networks for mobile communication, e.g. based on Ieee 802.11(b) and, in future, bluetooth technology, too.
   - Nowadays, security systems such as firewalls etc., are widespread, and the configurations of such systems usually afford a high level of security, which means

that it is extremely difficult, if not impossible, to defeat such systems in an attack. It is often easier and quicker to obtain the desired or necessary data by circumventing these systems in a direct **physical attack**. A physical attack can, for example, involve directly accessing data at a non-password protected workstation after gaining unauthorized access to the building and/or server rooms.

- People are frequently the weakest link in the security chain, which is why **social engineering** techniques that exploit inadequate security skills or insufficient security awareness are often successful. Such tests are appropriate after the introduction of a general security policy, for example, to assess the extent of its implementation and/or acceptance. False assumptions about the supposed effectiveness of a security policy often result in security risks that, provided that the situation is assessed accurately, can be mitigated by taking additional action. Sections 5.4 Ethical Issuesand 4.2 Legal Framework for Penetration Testing discuss in detail how far such tests can go.

6. **Starting point**: Where is the penetration test carried out from?

   The starting point of the penetration test, i.e. the point where the penetration tester connects his computer to the network or where his attacking attempts originate can be either inside or outside the client's network or building.

   - Most hacker attacks are staged via the network's connection to the internet. A penetration test from the **outside** is therefore able to detect and evaluate the potential risk of such an attack. Typically, the firewall, systems in the DMZ and RAS connections are investigated in such tests.
   - In a penetration test from the **inside**, the tester does not normally have to overcome firewalls or entry controls to access internal networks. Therefore a test from the inside can assess the effects of an error in the firewall configuration, a successful attack on the firewall, or of an attack by persons with access to the internal network.

3.5 Multistage Approach

In order to minimize risks, a combination of the different penetration tests shown in the classification is often advisable. For instance, a cautious, covert black-box test can be carried out from the outside in a first step, followed by an aggressive, overt white-box test from the inside. This approach combines the advantages of a black-box test - a realistic simulation of a genuine attack - with the benefits of a white-box test in terms of efficiency and damage limitation.

4 Legal Issues

The legal issues that have to be considered when conducting penetration tests can be subdivided into three types:

- Legal issues that can induce or motivate a business or a public authority to conduct a penetration test.
- Legal regulations and principles that the tester should observe when conducting penetration tests and which should be clarified with the client prior to testing.
- Legal aspects which form the basis of the contract between client and penetration tester.

4.1 Legal Reasons for Penetration Testing

While there are no laws that require a company or public authority to commission penetration tests, there are binding legal provisions relating to

- security handling and the availability of data relevant to tax and commercial law,
- treatment of personal data,
- the establishment and organization of an internal control system.

In order to protect company data, companies often take measures to guarantee the availability, confidentiality and integrity of data or to ensure access for authorized persons only. These mesaures include security concepts, authorization concepts and firewall systems. However, establishing these kinds of security systems is no guarantee that the legal requirements are met. Rather, the system's compliance with the legal requirements and stipulations must be checked for each invidual case. Penetration tests are a suitable means of verifying the effectiveness of such measures in certain areas.

The most important legal regulations which have to be observed when establishing and maintaining security and authorization systems are presented below in context for use in implementing penetration tests.

4.1.1 German Commercial Code (HGB)

Sec. 238 (1) of the German Commercial Code (HGB) stipulates that an entrepreneur keep his/her books in accordance with the Generally Accepted Accounting Principles (GoB) or in accordance with the Generally Accepted Principles of Computer-Assisted Accounting Systems (GoBS) (interpretive letter of the Federal Ministry of Finance to the supreme tax authorities of the states of November 7, 1995).

Section Four of the GoBS contains the regulations regarding the internal control system (ICS) of an enterprise:

- No. 4.1: "An ICS usually refers to all complementary and interconnected controls, measures and arrangements which serve the following purposes: securing and protecting existing assets and information from losses of all kinds. […]"

Section Five GoBS contains provisions relating to data security:

- No. 5.1: "The strong dependence of an enterprise on its stored information makes an in-depth data security concept essential for compliance with the GoBS. [...]"
- No. 5.3: "This information must be protected from loss and authorized modification. [...]"
- No. 5.5.1: "Information must be protected against unauthorized modification through effective access controls. [...]"

The provisions listed above illustrate the high demands on data security which are put on enterprises. These legal requirements can only be met by having an IT security concept (called "data security concept" in GoBS terminology) that is part of an internal control system. A penetration test can help verify on a sampling basis whether a security concept of this type meets the high legal requirements.

4.1.2 Law on Control and Transparency in Business (KonTraG)

Since the Law on Control and Transparency in Business (KonTraG) came into force in May 1998, management boards of stock corporations are required to establish a risk management system and carry out extended reporting to the supervisory board. Sec. 91 (2) of the German Stock Corporation Act (AktG) was revised as follows:

- Sec. 91 (2) AktG: "The management board must take appropriate measures; in particular, set up a monitoring system for early recognition of developments posing a risk to the going concern. [...]"

Due to the "spillover effect" this change in the regulations also applies to the management of a limited liability company (GmbH).

The legislation does not stipulate how such a risk management system should actually be set up. The Act does, however, state that a risk management system must contain elements such as an early warning system, an internal monitoring system including an audit and controlling. [Andersen99,

p. 20]. Here, penetration tests are an appropriate way of testing the IT-related part of the early warning system or parts of the audit.

4.1.3 German Banking Act (KWG)

Banks and other organizations in the financial services sector are subject to the regulations of the German Banking Act (KWG). One special feature of the German Banking Act is that the Federal Financial Supervisory Agency is entitled to conduct audits at all financial services institutions which may extend to all business areas of the company.

Sec. 44 (1) contains the following regulation:

- "[...] The Federal Financial Supervisory Agency may carry out audits at the institutions even if there is no special reason for them and transfer the execution of the audits to the Deutsche Bundesbank. [...]."

The area of internet security can be subject to an audit pursuant to Sec. 44 (1) KWG, particularly at banks which make their financial services available online.

It is therefore advisable that these banks carry out penetration tests before an audit of this kind in order to test the security of the internet applications used, identify vulnerabilities and issue recommendations on action for remedying any deficits.

4.1.4 Ordinances and Pronouncements of the Federal Financial Supervisory Agency (BAFin)

The Federal Financial Supervisory Agency (previously known as the Federal Banking Supervisory Office - BAFin) is legally authorized to issue ordinances and publish pronouncements that affect banks and other financial services providers that come under BAFin supervision. The following pronouncement is particularly interesting in relation to penetration testing:

"Statement Covering Minimum Requirements for the Trading Activities of Credit Institutions", which defines the requirements for the risk management system and the organization of the internal audit function.

It contains the following statements on the risk management system:

- No. 3.1 System Requirements: "[...] [The risk management system] should be incorporated into an overall risk monitoring and management structure covering as far as possible all the bank's areas of business and should facilitate the identification and analysis of comparable risks from nontrading activities. [...]"

- No. 3.4 Operational Risks: "[...] A written contingency planning has to ensure, among other things, that in the event of the breakdown of the technical equipment necessary for trading activities, back-up facilities can be deployed at short notice. In addition, precautions are to be taken to cope with possible software errors and with unforeseen staff absences. The procedures, documentation requirements, data processing systems and contingency plans in use for the trading activities are to be regularly reviewed."

Penetration testing puts a bank in a better position to judge the potential effects of an attack. They allow a definite statement to be made on the fuctionality of the risk mangement system.

The statement contains the following requirements in relation to the organization of the internal audit function:

- No. 5 Auditing: "Compliance with the minimum requirements is to be checked at irregular, appropriate intervals by the internal auditors. The main audit areas should be subjected to a risk-oriented audit at least once a year. Each subdivision of the minimum requirements is to be audited at least at three-yearly intervals; the audit rota is to be documented in an audit plan.

  The main audit areas are as follows:

  - Changes in the IT systems."

Penetration tests can provide effective support for risk-oriented monitoring of the main audit areas in an IT audit.

4.1.5 Federal Data Protection Act (BDSG)

Both state and federal law contain legal provisions relating to data protection, governing the treatment of personal data by public and non-public bodies.

In accordance with Sec. 1 II BDSG, the Federal Data Protection Act (BDSG) applies to the collection, processing and use of personal data by

1. public bodies of the Federation,
2. public bodies of the states, insofar as data protection is not governed by state legislation […],
3. private bodies insofar as they process or use data in data processing systems or in or from data files, or collect data for use in such systems or files […].

- Sec. 9 (1) BDSG technical and organizational measures: "Public and private bodies processing personal data either on their own behalf or on behalf of others shall take

the technical and organizational measures necessary to ensure the implementation of the provisions of this Act, in particular the requirements set out in the annex to this Act."

The annex referred to in this Act contains requirements relating to admission controls, access controls, relaying controls, input controls, task controls and availability controls.

- Sec. 9a BDSG data protection audit: "For improved data protection and data security, providers of data processing systems and programs and data processing bodies may have their data protection concept and their technical equipment tested and evaluated by independent and registered experts and publish the result of the examination. [...]"

Penetration tests can be used in a data protection audit as an efficient audit tool for asserting whether the regulations have been implemented and whether the data protection concept is effective.

Note: EU Data Protection Directive (95/46/EU)

The BDSG was amended on May 18, 2001 to implement the EU Data Protection Directive 94/46/EU in Germany.

Article 17 (1) of the Directive emphasizes the necessity of a security concept for companies in the EU: "Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. [...]"

An additional amendment to the BDSG is anticipated with the implementation of the European Data Protection Directive for Electronic Communication (2002/58/EU), which will lead to adjustments in the processing of personal data and protection of privacy in telecommunications in response to recent developments in the markets and technologies for electronic communication services.

- Article 4 (1) [security]: "The provider of a public electronic communications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. [...]"

The Directive provides for implementation by October 31, 2003 at the latest.

4.1.6 Treaty on Media Services (MDStV)

The Treaty on Media Services is aimed at creating a uniform framework for the various uses of information and communication services which are designed for a general audience.

The MDStV is mainly geared towards enterprises that offer media services commercially. A distinction is made between "distribution services" and "service providers". A distribution service is the provider of a media service (e.g. teleshopping). A service provider enables access to a media service. When an enterprise or an authority provides its employees with internet access it also becomes a service provider and must observe the regulations of MDStV.

The following paragraphs can be seen as relating to penetration tests from an auditing perspective:

- Sec. 13 (2) MDStV [provider's obligations]: "The provider of media services must make technical and organizational provisions to ensure that […] 3. the user can use media services protected from the knowledge of third parties. [...]"
- Sec. 17 MDStV [data protection audit]: "To improve data protection and data security, providers of media services can have their data protection concept and their technical equipment tested and evaluated by independent and registered experts and publish the result of the examination. [...]"

Penetration tests can be used specifically to test both the defined technical and organizational provisions and the data protection concept.

4.1.7 Teleservices Act (TDG) and Teleservices Data Protection Act (TDDSG)

The Teleservices Act is intended for services providers that "make their own teleservices or those of third parties available for use or provide access to their use." A teleservice is, for example, an individual communication service or an interactive ordering facility. As such, every organization that publishes information on an internet website, for example, or provides an e-mail contact address is a services provider.

The Teleservices Data Protection Act sets out a legal framework for data protection, within which services providers are permitted to collect, process and use the personal data of users.

- Sec. 4 (4) TDDSG [services providers' obligations]: "The services provider must make technical and organizational provisions to ensure that […] the user can use teleservices protected from the knowledge of third parties."

Here, penetration tests could likewise be used as a control tool for monitoring the effectiveness of the data protection concept.

4.1.8 The Telecommunications Act (TKG)

This Act is intended for commercial providers of telecommunications services. It mainly affects telephone companies and internet service providers. Companies in which employees use their telephone connection or their internet access at their workplace for private purposes are also deemed providers of telecommunications services and therefore fall under the scope of the Act. [LfDN99]

One of the objectives of the Telecommunications Act (TKG) is to maintain telecommunications secrecy in the field of telecommunications.

- Sec. 85 (2) TKG [telecommunications secrecy]: "Whosoever commercially provides or assists in the provision of telecommunications services shall be obliged to maintain telecommunications secrecy. [...]
- Sec. 87 (1) TKG [protective technical precautions]: "Whosoever operates telecommunications systems serving the commercial provision of telecommunications services shall take appropriate technical precautions or other measures with regard to telecommunications and data processing systems operated for such purpose in order to protect […]

  2. program-controlled telecommunications and data processing systems against unauthorized access, […]

  4. telecommunications and data processing systems against external attack and the effects of natural disasters."

Here too, penetration tests can be implemented to test the IT security concept.

4.1.9 Criminal Law

Computer crime has risen exorbitantly over the last few years. Overall, however, the possibilities for imposing sanctions under criminal law are limited and the creation of new criminal offenses has not yet led to any reduction in computer crime. The range of criminal offenses currently set out in German criminal law is meager and fails to offer any effective protection in terms of general crime prevention. In addition to this, it is often difficult to provide evidence of the offenses.

The provisions of the German Civil Code ["Strafgesetzbuch": StGB] that are relevant to computer crime are mainly in the sections "Violation of the Realm of Personal Privacy and Confidentiality", "Fraud and Breach of Trust", "Falsification of Documents" and "Damage to Property".

The following provides a summary of the criminal offenses which can be committed through unauthorized access to data processing systems.

- Sec. 202a (1) StGB [data espionage]: "Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine."

This criminal offense primarily protects all stored data and data in transfer against unauthorized access; the criminal act is the obtaining of data.

Section 263a StGB [computer fraud]: "Whoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the assets of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorized use of data or other unauthorized influence on the order of events, shall be punished with imprisonment for not more than five years or a fine."

The manipulation of a data processing procedure with the intent of obtaining for oneself or for a third person an unlawful material benefit is punishable. The criminal offense contained in Sec. 263a StGB further requires the offender to have acted intentionally and with the aim of obtaining an unlawful material benefit for himself or for a third person.

- Sec. 268 (1) StGB [falsification of technical recordings]: "Whoever, for purposes of deception in legal relations 1.) produces a counterfeit technical recording or falsifies a technical recording; or 2.) uses a counterfeit or falsified technical recording, shall be punished with imprisonment for not more than five years or a fine."

Pursuant to Sec. 268 (2) StGB, technical recordings refer to "a representation of data, measurements or calculations, conditions or sequences of events, which, in whole or in part, is produced automatically by a technical device, allows the object of the recording to be recognized either generally or by experts and is intended as proof of a legally relevant fact". The criminal offense of Sec. 268 (1) StGB is the production of a counterfeit technical recording, the falsification of a technical recording or the use of a counterfeit or falsified technical recording. However, to commit the criminal offense of Sec. 268 (1) StGB, the offender must also act in order to deceive in legal relations or, pursuant to Sec. 270 StGB, influence the data processing by means of falsification.

- Sec. 269 (1) StGB [falsification of legally relevant data]: "Whoever, in order to deceive in legal relations, stores or modifies legally relevant data in such a way that a counterfeit or falsified document would exist upon its retrieval, or uses data stored or modified in such a manner, shall be punished with imprisonment for not more than five years or a fine."

The above comments on Sec. 268 (1) StGB are also relevant here.

- Sec. 303a (1) StGB [alteration of data]: "Whoever unlawfully deletes, suppresses, renders unusable or alters data shall be punished with imprisonment for not more than two years or a fine."

These paragraphs make the unlawful deletion, suppression, rendering unusable or alteration of data punishable by law.

- Section 303b StGB [computer sabotage]: "Whoever interferes with data processing which is of material significance to the business or enterprise of another or a public authority by 1.) committing an act under Section 303a; or 2.) destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier, shall be punished with imprisonment for not more than five years or a fine."

4.1.10 European Convention on Cybercrime

The European Convention on Cybercrime was adopted by the Minister Committee of the European Council on November 8, 2001 with the aim of providing laws and procedures for the eradication of computer crime. It was signed by Germany and other member states of the European Council. It is, however, yet to be ratified.

Chapter Two of the Cybercrime Convention describes cases (measures to be taken at a national level) that a country must make punishable with regard to eradicating computer crime.

The parts of the Convention that are relevant for penetration testing are Titles 1 and 2 of Section 1 [substantive criminal law].

- Title 1: Offenses against the confidentiality, integrity and availability of computer data and systems

- Article 2: Illegal access/unauthorized intrusion into computer systems and networks
- Article 3: Illegal interception/unauthorized interception of network traffic
- Article 4: Data interference/unauthorized alteration of data
- Article 5: System interference/impairment or sabotage of computer systems
- Article 6: Misuse of devices/possession and misuse of systems and tools that are suitable for carrying out an action as in Article 2-5. This article does not, however, refer to the unauthorized use of security tools that are used for protective purposes, such as penetration tests.

- Title 2: Computer-related offenses
  - Article 7: Computer-related forgery
  - Article 8: Computer-related fraud

Article 6 of the Convention makes particularly clear that the authorized use of hacker and security tools does not conflict with the purpose of the article. Neither does the Cybercrime Convention intend to hinder the work of a penetration tester by making his activity punishable under law. However, the Convention is yet to be implemented in German law.

4.2 Legal Framework for Penetration Testing

During a penetration test, the tester carries out actions that, if performed without the client's consent, may contravene present law.

4.2.1 Criminal Law

The penetration tester will usually not commit a criminal offense since he does not act with the necessary intentions – such as that of unlawful enrichment. Moreover, such acts of intrusion, the content and scope of which has been agreed on with the client, is justified by the approval of the latter.

The exact definition of the scope of action by the client and the tester is therefore decisive (cf. 4.3.3 "Subject of the agreement"). Once the actual scope of action has been defined, it is helpful to obtain the necessary approval in the form of a separate declaration by the client prior to commencing testing.

The following provisions are also significant with regard to the client's approval:

Access Control Services Protection Act (ZKDSG)

The ZKDSG regulates the protection of access-controlled services and access control services. An access-controlled services is, among other things, a teleservice within the meaning of Sec. 2 TDG or a media service within the meaning of Sec. 2 MDStV. An access control service is a technical process or facility that enables the authorized use of an access-controlled service.

By adopting this law, the legislator wanted to guarantee the protection of fee-attracting services such as pay TV against the unauthorized manipulation of security mechanisms.

- Sec. 3 ZKDSG [prohibition of commercial intervention to circumvent access control services]: "1.) The production, import and distribution of circumvention facilities for commercial purposes, 2.) the possession, technical installation, maintenance and exchange of circumvention facilities for commercial purposes and 3.) the promotion of circumvention facilities are prohibited."

An access-controlled service is, for example, a password-protected WWW or FTP server. The purpose of a penetration test is to circumvent an existing security mechanism. This means that as soon as tools are used to perform the penetration test (circumvention facilities), an infringement of the ZKDSG is unavoidable. A penetration tester will also normally fulfill the criterion of the use of hacker and security tools for business purposes. Accordingly, a penetration tester who has an exploit for remotely accessing a password-protected web server could be committing an offence and may face a fine of up to EUR 50,000. [Emmert02, p.6] In such cases it is advisable to obtain the relevant permission from the authorized user in case of any acts that could constitute a criminal offense.

The Telecommunications Act (TKG)

The following provisions of the TKG could be relevant for a penetration tester:

- Sec. 65 (1) [abuse of transmitting equipment]: "It shall be prohibited to own […] transmitting equipment […] which, by its form, simulates another object […] and, due to such circumstances, is particularly suitable to intercept the non-publicly spoken words of another person without such person detecting this."

- Sec. 86 TKG [prohibition to intercept, obligation of operators of receiving equipment to maintain secrecy]: "Interception by means of radio equipment of messages not intended for that radio equipment shall not be permitted. [...]"

These regulations prohibit actions that are performed during penetration tests, such as the use of network sniffers for intercepting network traffic, unless the authorized user has given his/her prior permission.

Proposal for a Council Framework Decision on Attacks Against Information Systems

On April 19, 2002, the European Commission issued a proposal for a Council Framework Decision on attacks on information systems. The framework decision is aimed at bringing in line the various member states' criminal law provisions for attacks on information systems and improving cooperation between the authorities.

It comprises 14 articles, of which articles 3 and 4 contain details on criminal offenses:

- Article 3 [illegal access to information systems]: "Member States shall ensure that the intentional access, without right, to the whole or any part of an information system is punishable as a criminal offence where it is committed 1.) against any part of an information system which is subject to specific protection measures; or 2.) with the intent to cause damage to a natural or legal person; or 3.) with the intent to result in an economic benefit."
- Article 4 [illegal interference with information systems]: "Member States shall ensure that the following intentional conduct, without right, is punishable as a criminal offence:
  (a) the serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data;
  (b) the deletion, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system where it is committed with the intention to cause damage to a natural or legal person."

Further developments in the framework decision remain to be seen. However, we can already say that a penetration tester who acts at the consent of his client and remains within the scope of action defined by the client, will remain unpunishable after the framework decision has come into force since he will normally lack the intention to commit a punishable act or his act would be justified due to the approval of the authorized user.

4.2.2 Works Constitution Act (BetrVG)

If a company that commissions a penetration test has a works council, it should be noted that the works council has a right to be informed (Sec. 80 II BetrVG). With respect to the regulation in Sec. 87

(1) No. 6 BetrVG, the works council should be involved in the planning of the penetration testing process.

- Sec. 87 (1) No. 6 BetrVG [rights of codetermination]: "The works council shall […] codetermine on the following matters:
  - the introduction and application of technical equipment for monitoring the behavior or performance of the employees."

The purpose of penetration tests is to check the effectiveness of existing security facilities. A penetration test can also serve as a tool for assessing the performance of employees. For example, social engineering techniques are used explicitly to examine the behavior of employees.

But even when it is not the main purpose of a penetration test to monitor or assess the performance of employees, the results of a penetration test are generally suited to doing just that. According to the Federal Labor Court ("*Bundesarbeitsgericht"*), what is decisive is whether or not the equipment is objectively suitable for monitoring, regardless of whether the employer pursues this objective and actually evaluates the data obtained in the monitoring process. We strongly recommend involving the works council at an early stage, even when its approval is not required for certain test procedures.

4.3 Important Terms in Contracts Between Penetration Tester and Client

4.3.1 What Type of Contract is a Penetration Test Contract?

A penetration test is normally a service for remuneration. As opposed to a contract for work and services, the agreed service only is due, but no particular economic outcome.

4.3.2 General Terms and Conditions

If the tester has general terms and conditions, these must be included in the contract. The client must have been made aware of them and agree to their validity.

4.3.3 Subject of the Contract

In addition to the purpose of the penetration test, the parties must define in the contract the nature and scope of the tools and techniques to be used.

Key elements of the subject of the contract are:

- 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.

There is a detailed overview of possible objectives in section 3.2 of this study "Objectives of penetration testing".

- Nature of the penetration test

  Reference should be made to the type of penetration test to be performed (see section 3.4 of this study "Classification"). The following classification criteria may be used:

  - Information base (black-box or white-box test)
  - Aggressiveness (passive/scanning to aggressive)
  - Scope (full, limited or focused)
  - Approach (covert or overt)
  - Technique (network-based, other communications, physical access, social engineering)
  - Starting point (from the outside or the inside)

  By making these kinds of specifications the tester avoids unnecessary misunderstandings and risks right from the start and ensures that the penetration test is tailored to the client's needs. In addition, the scope of the client's approval, which should be obtained as a precaution from a criminal law perspective, is defined.

- 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.

4.3.4 Client

Particularly concerning the approval required for taking potentially damaging measures during the testing process, it is important that the contract is signed by a legal representative of the client. This means that only a person authorized to represent him, e.g. for a trading company, the general manager, an authorized signatory or another person with a similar individual authorization, such as the head of the IT department, may commission the performance of the penetration test.

Before performing the penetration test, the penetration tester should request appropriate evidence to satisfy himself that the client's representative is authorized to represent him.

4.3.5 Tester

If the tester intends to contract out parts of the test, an "opening clause" should be included in the contract. However, since areas relevant to security are affected, the client will not normally agree to this kind of opening clause. It is therefore helpful to name the subcontractor when the contract is concluded. This ensures that only these persons are authorized to perform the test procedures. Appointing executing parties is particularly important when unconventional testing procedures such as social engineering or the circumvention of physical security measures have been planned, since this protects both parties and helps avoid misunderstandings.

4.3.6 Written Form

All terms of the contract must be agreed in writing. In addition, the parties should expressly agree to a requirement of writing, which should cover all subsidiary agreements.

4.3.7 The Client's Obligations

In the interests of the penetration tester, the contract should set out the client's legal duty to cooperate in as much detail as possible. The following elements should be taken into account:

- 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 where this has not already been done in fulfillment of the Generally Accepted Principles of Computer-Assisted Accounting Systems (GoBS). Data backups ensure that the data can be recovered if necessary and mitigate the potentially adverse effects of data loss.

4.3.8 The Tester's Obligations

In the client's interests, the tester should be assigned the following obligations:

- 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.

- 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.

4.3.9 Execution of the Contract

A start and finish date should be specified for the contract. The penetration test must be carried out within this period of time. This ensures that penetration attempts which occur after this period can be clearly identified as real attacks by third parties, thus avoiding any misunderstandings. It should be noted that the penetration tester is authorized to perform his tests in the agreed period of time only.

4.3.10 Special Right to Terminate

During the course of penetration testing, circumstances may arise which could hinder the progress of the tests (for example, a crucial system crashes and necessitates extensive manual tidying-up work). A

special right to terminate can be included in the contract for cases such as these. In addition, the general rules for terminating contracts for services apply, particularly Sec. 627 (2) BGB.

4.3.11 Limitation of Liability

When the parties are agreeing on limitations of liability, they should note that a limitation of liability can only be legally agreed to within the limits of the General Terms and Conditions of Trade Act (AGB-Gesetz). A limitation of the tester's liability for gross negligence and intent and a disclaimer of liability for damages resulting from defects or indirect damage are normally possible as long as there is no culpable infringement of a significant contractual obligation.

5 General Requirements

In addition to the legal framework, there are a number of general requirements pertaining to organization, personnel and technical matters for the performance of penetration tests.

5.1 Organizational 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 online

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 coutermeasures. 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.

5.2 Personnel Requirements

Penetration tests must be tailored to the client's individual situation and thus do not lend themselves well to standardization. Therefore, a penetration test can only follow a rigid pattern to a certain extent. As such, penetration tests should only be performed by persons with many years of experience in IT security.

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 (for firewalls see e.g. [BSI01]).

- 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, Lophtcrack for Windows passwords). Commercial tools can be used for performing an efficient test and freeware 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 unsystematic or even chaotic test which is not subsequently traceable.

5.3 Technical Requirements

The following technical requirements must be met before the penetration tester can perform the test procedures:

- Access to public networks

  Access to the internet or the public telephone network is an important precondition for performing the penetration test since most attacks are launched over these communication channels. A sufficiently high-capacity internet connection should therefore be available. Here it is important to note that vulnerability scanners in particular require a high bandwidth. The efficiency of testing therefore depends for one thing on the available line capacity .

- Availability of suitable auditing tools

  The penetration tester must have suitable tools at his disposal for performing the tests. Many of these tools can be downloaded from the internet free of charge. Tools such as vulnerability scanners, however, often attract extremely high royalties (usually depending on the number of IP addresses to be scanned). An efficient test requires the “right” tools rather than large numbers of tools. The tester knows the effects and side-effects of the tools and is often able to assess a large number of results quickly and differentiate false statements from true ones.

- Local test network

  The various tools must be tested in a local test network before use in a real penetration test. These kinds of tests also allow the penetration tester to familiarize himself with hacker tools and vulnerability scanners and with the results they produce. If the systems of the test network are suitably configured, they also allow vulnerabilities in the systems to be tested and verified.

5.4 Ethical Issues

In addition to the conditions outlined above, there are also a number of ethical issues that need to be considered before starting penetration testing. The parties should, for one thing, clarify whether and to what extent the use of social engineering techniques is justified. They should also discuss whether vulnerabilities that have been identified as such in a penetration test need to or may be exploited.

First, however, the parties should make quite clear that a penetration test can ever only be a commissioned activity. Any proactive behavior, i.e. launching an attack attempt without a mandate should always be considered an attack and is to be rejected.

5.4.1 The Use of Social Engineering Techniques

The following gives an outline of why social engineering is so successful in order to decide whether the use of such techniques is justified in a penetration test. The 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. [Kabay00]

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.

5.4.2 Exploiting Vulnerabilities

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.

6 A Penetration Testing Methodology

This chapter introduces a methodology for penetration testing, divided into five phases. This methodology takes account of the issues discussed above and was developed for general applicability. The methodology is based on a structured procedure for performing penetration tests which acts as a basis for devising individual action plans for specific penetration tests.

6.1 Requirements for a Penetration Testing Methodology

The methodology describes and structures the performance of a commissioned penetration test. A test should always be receptive to the client's objectives and care must be taken not to neglect this perspective. This means, for example, outlining the test steps required to achieve this objective or explaining whether a penetration test is suitable for achieving them at all. A methodology should also include measures for complying with the legal provisions (see e.g. [ISACA_CH99]) and for observing the conditions regarding organization and personnel for performing penetration tests. It should take account of the limited time available and must include an assessment of the potential risk or a cost-benefit analysis.

A module-based approach such as the OSSTMM [Herzog02] is advisable for grouping individual test steps since this allows the steps involved in a penetration test to be categorized thematically. This gives the test a clear framework and also allows the tester to devise a suitable penetration test by selecting or excluding certain modules.

For financial reasons, an actual penetration test will not normally make use of all possible test modules. While this would ensure a fully comprehensive test, it would also be extremely time-consuming and thereby be neither reconcilable with the client's objectives nor with specific security requirements. When security requirements are particularly high, the test should be as comprehensive as possible. This means that all or most modules must be applied and all of the client's systems must be included in the test. If security requirements are low, certain modules can be left out and/or only exposed or externally visible systems tested. Financial considerations should determine the scope of the penetration test. The costs and risks of the testing activities must be weighed up against the potential costs and risks which could be incurred in the event of an attack.

6.2 The Five Phases of a Penetration Test

The following introduces the five phases of a penetration test based on the considerations outlined above. The individual phases take place successively:

Phase 1: Preparation; it is difficult to fulfill the client's expectations without thorough preparation, such as reaching an agreement on the objectives of the penetration test. 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.

Phase 2: Reconnaissance; after the objectives, scope, procedures, emergency measures etc have been defined taking account of the legal and organizational aspects and other conditions, the tester can start gathering information on the target. 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 abovementioned test lasting several weeks.

Phase 3: Analyzing information and risks; a successful, transparent and economically efficient procedure must analyze 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 in phase 4 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.

In a penetration test for which the number of target systems has been clearly defined in phase 2, this selection means that the number of target systems for phase 4 is automatically reduced.

The restrictions 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.

Phase 4: 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.

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 will be continued.

Phase 5: Final analysis; as well as the individual test steps, the final 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.

6.3 Approach

Figure 2 illustrates a five-phase approach to penetration testing. 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.

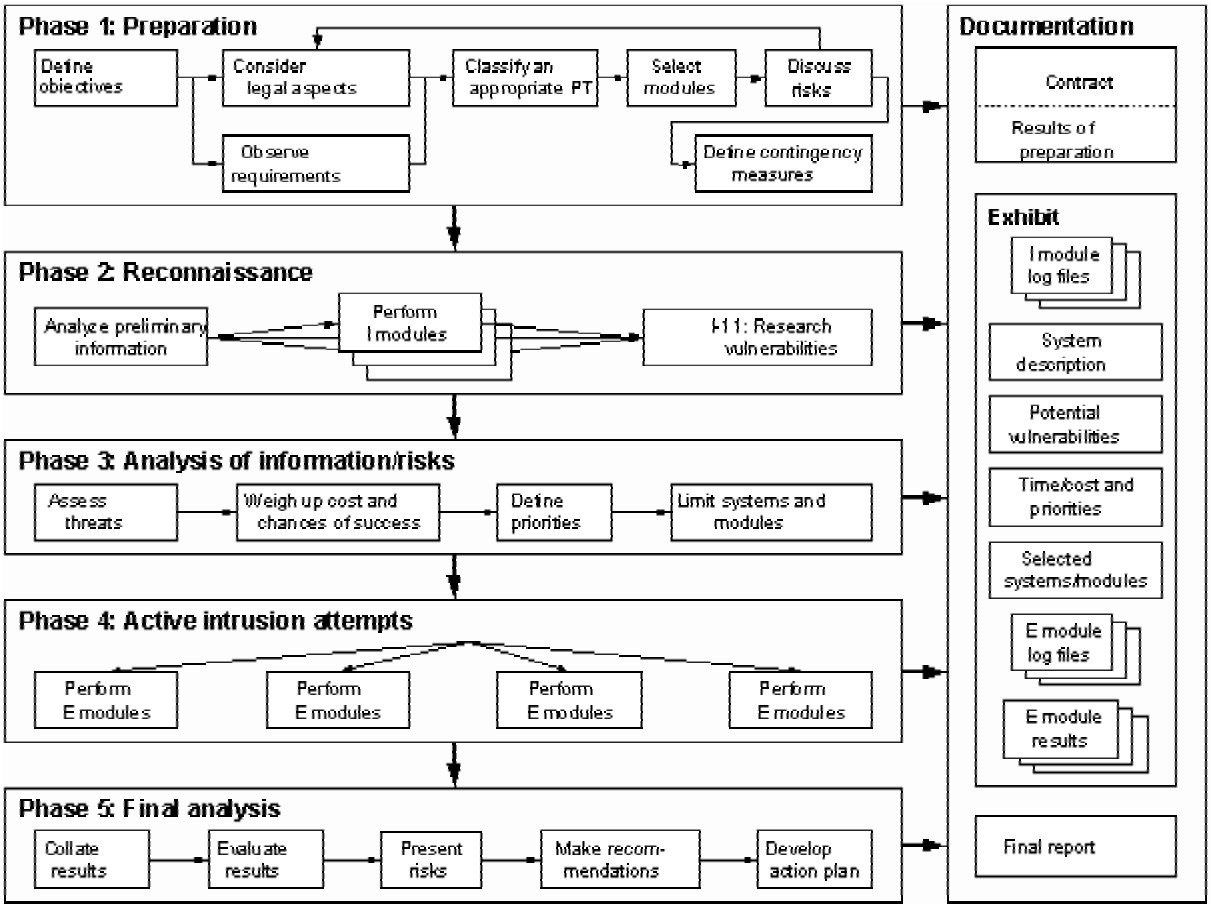


Figure 2: Five-phase penetration testing procedure

In spite of attempts to keep the methodology as general as possible, situations may arise in practice which call for deviations from the procedure detailed here. All steps taken that deviate from the methodology detailed here should be documented and justified separately.

6.4 Modules for the Test Procedures

The approach described above does not contain explicit test procedures, it mentions only the performance of I and E modules. Based on the OSSTMM [Herzog02], the different testing procedures which can be carried out in a penetration test have been grouped together in modules. The test objects are only accessed in phase 2 – "Reconaissance" and phase 4 – "Active intrusion". The modules have been divided into two classes accordingly, **I modules** for reconnaissance and **E modules** for penetration attempts. The modules have been divided up so that each of the steps belong to the same values of penetration testing classification criteria. The performance of port scans, for example, is divided into a module for covert port scans and a module for overt port scans, and the firewall testing is divided into modules for testing from the outside and from the inside.

6.4.1 Reconnaissance Modules

Table 1 contains a list of the reconnaissance modules I 1 to I 22. The testing steps contained in the modules are described in Section 6.5.1 and the equivalent OSSTMM modules are listed in the appendix (**A.6.1**).

No.	*Module*
I 1	**Analysis of Published Data**
I 2	**Covert Queries of Basic Network Information**
I 3	**Overt Queries of Basic Network Information**
I 4	**Stealthy Port Scans**
I 5	**Noisy Port Scans**
I 6	**Application Identification**
I 7	**System Identification**
I 8	**Covert Router Identification**
I 9	**Overt Router Identification**
I 10	**Covert Firewall Identification**
I 11	**Overt Firewall Identification**
I 12	**Vulnerability Research**
I 13	**Application Interface Identification**
I 14	**Collecting Information for Social Engineering**
I 15	**Collecting Information for Computer-Based Social Engineering**
I 16	**Collecting Information for Personal Social Engineering**
I 17	**Wireless Communications Testing (Scanning Only)**
I 18	**Telephone System Testing (Identification)**
I 19	**Voicemail System Testing (Identification)**
I 20	**Fax System Testing (Identification)**
I 21	**Analysis of Physical Environment**
I 22	**Access Control Identification**

Table 1: List of reconnaissance modules

6.4.2 Modules for Active Intrusion Attempts

Table 2 is a list of the modules E 1 to E 23 for active intrusion attempts. The testing steps contained in the modules are described in 6.5.2 and the equivalent OSSTMM modules are listed in the appendix (**A.6.2**).

No.	*Module*
E 1	**Covert Verification of Actual Vulnerabilities**
E 2	**Overt Verification of Actual Vulnerabilities**
E 3	**Overt Queries of Basic Network Information**
E 4	**Covert Router Testing**
E 5	**Overt Router Testing**
E 6	**Test of Trust Relationships Between Systems**
E 7	**Covert Firewall Test From Outside**
E 8	**Overt Firewall Test From Outside**
E 9	**Testing the Firewall From Both Sides**
E 10	**IDS System Testing**
E 11	**Intercepting Passwords**
E 12	**Password Cracking**
E 13	**Test of Susceptibility to Denial of Service Attacks**
E 14	**Computer-Based Social Engineering**
E 15	**Direct, Personal Social Engineering With Physical Access**
E 16	**Indirect, Personal Social Engineering Without Physical Access**
E 17	**Wireless Communications Testing**
E 18	**Testing Administrative Access to the Telephone System**
E 19	**Voicemail System Testing**
E 20	**Testing Administrative Points of Access to the Fax System**
E 21	**Modem Testing**
E 22	**Active Test of Access Controls**
E 23	**Test of Escalation Procedures**

Table 2: List of modules for active intrusion attempts

6.4.3 Extendability

If future developments demand new testing steps, the list of modules can be extended. All steps to be performed in a new module must belong to the same classification criteria otherwise, due to the exclusion principle, the module cannot be integrated into the methodology.

6.4.4 Exclusion Principle

The modules are selected according to a negative exclusion principle rather than a positive selection principle. Based on the selected classification, the modules which cannot be performed due to the selected approach are excluded from the tests. If a module is not excluded, the test steps contained in it must be carried out, which helps to ensure a comprehensive penetration test. If a module is to be excluded for other reasons, these reasons must be set out and documented.

After the objectives of the penetration test have been defined, the appropriate test is selected using the classification system (see Section 3.4) and taking account of the legal and organizational aspects. The chosen classification then determines via the exclusion principle which modules for reconnaissance and for active penetration cannot be performed. The classification system is shown again in Figure 3, stating the modules to be excluded for each of the criteria.

The choice of information base – white-box or black-box – does not directly affect the choice of modules. However, in a white-box test, depending on the documents available, a number of test procedures can be discarded and replaced by “reading up”.

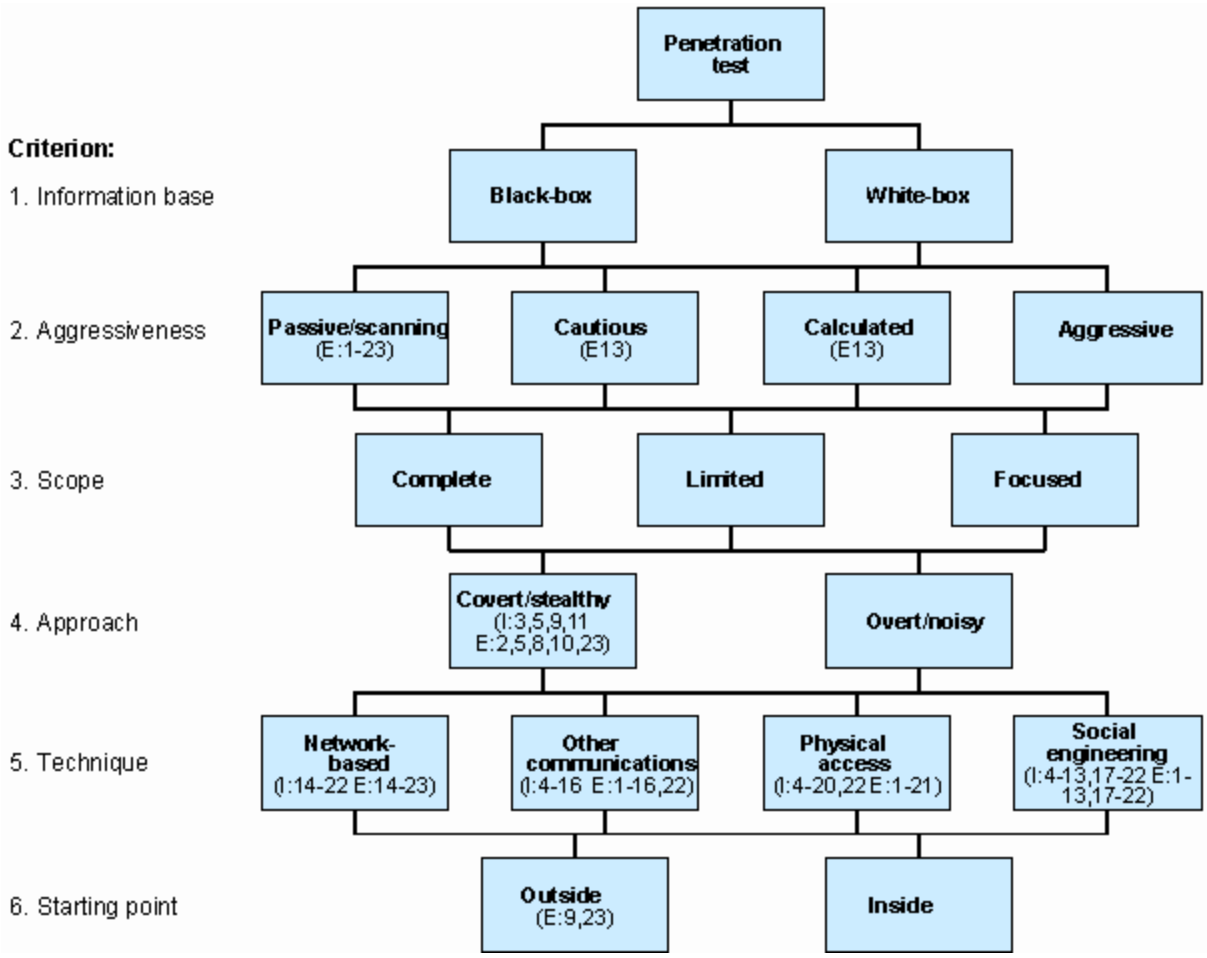


Figure 3 : Exclusion of modules based on classification

This procedure is illustrated below. If, for instance, the following penetration test is to be performed:

Criterion	Value	Excluded I modules	Excl. E modules
1. Information base:	**black-box**	-	-
2. Aggressiveness:	**cautious**	-	E 13
3. Scope:	**focused**	-	-
4. Approach:	**covert**	I 3, 5, 9, 11	E 2, 5, 8, 10, 23
5. Technique	**network-based**	I 14-22	E 14-23
6. Starting point:	**from the outside**	-	E 9, 23

I modules 3, 5, 9, 11, 13-22 are excluded, as are E modules 2, 5, 6, 8-10, 14-23. The remaining modules must be performed in the penetration test.

6.5 Module Descriptions

6.5.1 Description of Reconnaissance Modules

This section outlines the descriptions of the reconnaissance modules I 1 to I 22. Each module includes a brief description, the expected results, the requirements, the testing steps to be performed, and the associated risks.

I 1. Analysis of Published Data	
The tester tries to obtain as much information as possible about the target organization. In particular, he attempts to gather information about the company, its employees and the technology used.	
Expected results:	**Done**
• Company profile	☐
• Profile of employees	☐
• Survey of the technology used by the organization	☐
• Survey of the organization's partnerships and strategies	☐
Requirements:	
None	
Test steps:	**Effort**
• Search for information on the organization's homepage	low
• Research in public databases	low
• Research relevant information in news groups	medium
Risks:	
None	

I 2. Covert Queries of Basic Network Information	
Basic information about the network to be tested as a basis for a penetration test is obtained in stealthy or covert queries.	
Expected results:	**Done**
• Domain names	☐
• IP address ranges	☐
• Host names	☐
• IP addresses	☐
• Description of server functions	☐
• ISP information	☐
• Contact partners (admin-c)	☐
Requirements:	
IP address/IP range or domain/server names	
Test steps:	**Effort**
• Query public databases (Whois, Ripe, Arin)	low
• Query name servers (caution is required as attempted zone transfer could be detected)	medium
• Examine information in e-mail headers	low
• Scan HTML information of the websites offered to find external links or comments	medium
• Scan news groups for postings by the target organization's employees	low
• Scan the target organization's job vacancies for information about the IT environment	low
Risks:	
None	

I 3. Overt Queries of Basic Network Information	
Basic information about the network to be tested is gathered as a basis for a penetration test.	
Expected results:	**Done**
• Domain names	☐
• IP address ranges	☐
• Host names	☐
• IP addresses	☐
• Description of server functions	☐
• ISP information	☐
• Contact partners (admin-c)	☐
Requirements:	
IP address/IP range or domain/server names	
Test steps:	**Effort**
• Query public databases (Whois, Ripe, Arin)	low
• Query name servers, with a zone transfer attempt	low
• Ping scan of the IP range, neighboring IP addresses and common host names	low
• Examine information in e-mail headers	low
• Scan websites to find internal links or comments	medium
• Scan news groups for postings by the target organization's employees	low
• Scan the target organization's online/offline job vacancies for information about the IT environment	low
Risks:	
None	

I 4. Stealthy Port Scans	
A stealthy port scan is run on all identified devices in order to identify which services each device offers, with which operating system.	
Expected results:	**Done**
• Information on the services offered by the device	☐
• Identification of the operating system	☐
Requirements:	
Knowledge of basic network information	
Test steps:	**Effort**
• Perform a port scan that is impossible or difficult to detect, e.g. by setting suitable parameters when using port scanning tools or by making queries at long intervals.	medium
Risks:	
The port scan could be detected.	

I 5. Noisy Port Scans	
A port scan is run on all identified devices in order to identify which services each device offers, and with which operating system.	
Expected results:	**Done**
• Information on the services offered by the device	☐
• Identification of the operating system	☐
Requirements:	
Knowledge of basic network information	
Test steps:	**Effort**
• Perform a normal port scan.	medium
Risks:	
None	

I 6. Application Identification	
The tester attempts to identify applications and services that can be accessed over the internet.	
Expected results:	**Done**
• Identification of server services offered (e.g. HTTP, FTP, NNTP)	☐
• Identification of applications offered (e.g. web mail, online banking, e-commerce software)	☐
Requirements:	
Results from a previous port scan.	
Test steps:	**Effort**
• Evaluate the results of the port scan	medium
• Identify publicly available internet applications, such as online banking	low
Risks:	
None	

I 7. System Identification	
The tester attempts to obtain information about the operating system, the patch level status and the system's hardware.	
Expected results:	**Done**
• Information about the operating system	☐
• Information about the patch level status	☐
• Information about the hardware	☐
Requirements:	
Knowledge of basic network information	
Test steps:	**Effort**
• Perform a port scan with system detection/IP packet analysis	medium
• Analyze banner information	medium
Risks:	
The systems could crash or their performance could be impaired.	

I 8. Covert Router Identification	
The tester attempts to identify the routers used by the target organization, their functionality within the network as well as the operating system used, the manufacturer and the router model by making stealthy or covert queries.	
Expected results:	**Done**
• IP addresses of the routers	☐
• Function of the routers in the network	☐
• Operating system, manufacturer and router model	☐
Requirements:	
Knowledge of basic network information Results of the stealthy port scans and system identification	
Test steps:	**Effort**
• Trace routes cautiously with a “trace route” command	medium
• Analyze the routed IP packets	medium
Risks:	
The attempt to identify routers could be detected.	

I 9. Overt Router Identification	
The tester attempts to identify the routers used, their role within the network and the operating system of the routers used by the target organization.	
Expected results:	**Done**
• IP addresses of the routers	☐
• Role of the routers in the network	☐
• Operating systems of the routers	☐
Requirements:	
Knowledge of basic network information. Results of the noisy port scans and system identification	
Test steps:	**Effort**
• Trace routes using a “trace route” command	medium
• Analyze the routed IP packets	medium
Risks:	
None	

I 10. Covert Firewall Identification	
The tester attempts to identify the firewalls: o type/form (packet filter, dual or single-homed, application gateway etc.) o model (manufacturer, version, configuration access, etc.) o configuration (open ports, open protocols, etc.)	
Expected results:	**Done**
• IP addresses and/or DNS names of the firewall components (firewall hosts, application gateway, etc.)	☐
• Firewall operating systems	☐
• IP addresses of other components of the firewall configuration (internal and external routers)	☐
• Model and patch level of the firewall software	☐
Requirements:	
Knowledge of basic network information, results of stealthy port scans	
Test steps:	**Effort**
• Banner lookup of the firewall components	low
• Direct port scan of the firewalls	medium
• Trace routes using a “trace route” command	medium
Risks:	
The attempt to identify the firewalls could be detected.	

I 11. Overt Firewall Identification	
The tester attempts to identify the firewalls: o type/form (package filter, dual or single-homed, application gateway, etc.) o model (manufacturer, version, configuration access, etc.) o configuration (open ports, open protocols, etc.)	
Expected results:	**Done**
• IP addresses and/or DNS names of the firewall components (firewall hosts, application gateway, etc.)	☐
• Firewall operating systems	☐
• IP addresses of other components of the firewall configuration (internal and external routers)	☐
• Model and patch level of the firewall software	☐
Requirements:	
Knowledge of basic network information, results of noisy port scans	
Test steps:	**Effort**
• Banner lookup of the firewall components	low
• Direct port scan of the firewalls	medium
• Trace routes using a “trace route” command	medium
Risks:	
None	

I 12. Vulnerability Research	
The obtained information (open ports, applications, operating systems) is analyzed for vulnerabilities, with a range of tools being used.	
Expected results:	**Done**
• Extended list of the patch levels of systems and applications	☐
• List of potential vulnerabilities	☐
Requirements:	
In-depth knowledge of open ports, services offered, applications and operating systems used.	
Test steps:	**Effort**
• Use state of the art vulnerability scanners (see A.7)	medium
• Query up-to-date vulnerability databases (see A.7)	medium
• Scan mailing lists/underground FTP archives, IRC servers and news groups on hacking/exploits	high
Risks:	
The use of vulnerability scanners can cause the devices being tested or the network components used to crash or have other adverse effects on them.	

I 13. Application Interface Identification	
The interfaces which have been identified and can be accessed on the internet, particularly those between self-developed systems, are examined for potential vulnerabilities. This can involve DMZ applications, which can access applications in the company network via an interface (e.g. accessing the system with online transactions) and applications within the company network.	
Expected results:	**Done**
• List of potential vulnerabilities the application interfaces (e.g. web servers, ERP system).	☐
• Knowledge about any existing interfaces between the different applications.	☐
Requirements:	
Information on the applications and systems used, the results of the port scans	
Test steps:	**Effort**
• Scan the services offered on the homepage, such as database queries, for potential vulnerabilities.	high
Risks:	
None	

I 14. Collecting Information for Social Engineering	
Obtaining information for social engineering, provided either knowingly or unknowingly by the organization.	
Expected results:	**Done**
• Identification of the relevant departments	☐
• List of people who work in the relevant departments	☐
• Names, job descriptions, e-mail addresses of potential target persons	☐
• Organizational charts of the target organization showing the different hierarchical levels and management positions (heads of department, etc.)	☐
• Form of e-mail addresses, internal mailing lists and typical senders of internal mailings	☐
Requirements:	
Company name, name of the institution	
Test steps:	**Effort**
• Analyze information on the target organization's website.	low
• Analyze information in the press or databases	high
• Search news groups for e-mail addresses of employees and applications of the target organization published in postings	medium
Risks:	
None	

I 15. Collecting Information for Computer-Based Social Engineering	
Obtaining information for computer-based social engineering, provided either knowingly or unknowingly by the organization.	
Expected results:	**Done**
• List of IT systems and IT applications used in the different departments	☐
Requirements:	
Results of I 14: Information on departments/people/the organization, etc.	
Test steps:	**Effort**
• Analyze the target organization's website for information on operating systems and applications	low
• Search the organization's job vacancies for information about its IT systems	high
• Research support forums for postings by the target organization's employees	medium
• Identify the e-mail programs of the target organization/employees on the basis of headers	low
Risks:	
None	

I 16. Collecting Information for Personal Social Engineering	
Obtaining information for personal social engineering, provided either knowingly or unknowingly by the organization.	
Expected results:	**Done**
• List of the service companies that work for the target organization	☐
• List of the target organization's major customers	☐
• Information on the location of the different departments within the buildings	☐
Requirements:	
Results of I 14: Information on departments/people/the organization, etc.	
Test steps:	**Effort**
• Analyze the contact information on the target organization's website	low
• Analyze the contact or customer information in the press or databases	medium
• Observe the target organization's building	high
• Identify service companies by making telephone inquiries	medium
Risks:	
None	

I 17. Wireless Communications Testing (Scanning Only)	
The tester checks whether a WLAN is operated. If the existence of a WLAN is verified, the key data is collected.	
Expected results:	**Done**
• Verification of the existence of a WLAN	☐
• Identification of the model and the points of access to the WLAN	☐
• Type of connection (authenticated or nonauthenticated)	☐
• Geographic spread of the WLAN	☐
• Examination of the use and type of encryption technology	☐
Requirements:	
None	
Test steps:	**Effort**
• Attempt to connect to the WLAN	medium
• Intercept traffic on the WLAN	high
• War walking/war driving (to determine the spread of the WLAN)	medium
Risks:	
None	

I 18. Telephone System Testing (Identification)	
The tester attempts to identify the type of telephone system and how to access it.	
Expected results:	**Done**
• Identification of the telephone system	☐
• Identification of the remote access points for maintenance purposes	☐
Requirements:	
Number range	
Test steps:	**Effort**
• Place test calls to telephone numbers with the target organization's number range	medium
• Analyze the signals of the telephone system	very high
• Search the product documentation of the telephone system for preset maintenance access numbers/standard passwords	medium
Risks:	
None	

I 19. Voicemail System Testing (Identification)	
The tester attempts to find out whether a mailbox system is being used. If the existence of a mailbox system can be verified, further information is collected.	
Expected results:	**Done**
• Verification of the existence of a mailbox system	☐
• Verification of the possibility of accessing the mailbox from the public telephone network	☐
• List of the accessible mailboxes identified	☐
Requirements:	
None	
Test steps:	**Effort**
• Place test calls to telephone numbers with the target organization's number range	medium
• Search the product documentation of the telephone system for details of the mailbox system	medium
Risks:	
None	

I 20. Fax System Testing (Identification)	
The tester attempts to find out which fax machines are used by the target organization and which systems control them	
Expected results:	**Done**
• List of the fax machines	☐
• List of the systems that control the fax machines and their operating systems	☐
Requirements:	
Telephone number range(s)	
Test steps:	**Effort**
• Place test calls to telephone numbers with the target organization's number range	medium
• Use a war dialer with system identification components	high
• Search product documentation of the fax machines for external maintenance access points	medium
Risks:	
The attack could be detected.	

I 21. Analysis of Physical Environment	
The area surrounding the company premises is examined with regard to organizational processes and interfaces.	
Expected results:	**Done**
• Map of building/surrounding area	☐
• List of visible rooms	☐
• List of rooms which could be bugged (with electroacoustic or video devices)	☐
• List of organizational processes (deliveries etc.)	☐
Requirements:	
None	
Test steps:	**Effort**
• Observe company premises and the surrounding area	medium
• Observe procedures for delivery, cleaning, visitors, etc.	high
Risks:	
None	

I 22. Access Control Identification	
The access controls to the company premises and critical areas (e.g. computer center, server rooms) as well as the possibilities for circumventing these are identified.	
Expected results:	**Done**
• List of ways to gain access	☐
• List of access controls in place	☐
• Authentification procedure for members of the organization and guests	☐
• Ways of circumventing the security measures	☐
Requirements:	
Map of the building/site	
Test steps:	**Effort**
• Observe company premises and the surrounding area	medium
• Analyze access controls with a view to effectiveness and ways of circumventing them	high
Risks:	
None	

6.5.2 Description of Active Intrusion Modules

This section describes the modules for active intrusion attempts, E 1 to E 23. Each module includes a brief description, the expected results, the requirements, the testing steps to be performed, and the associated risks.

E 1. Covert Verification of Actual Vulnerabilities	
The actual threat potential of the vulnerabilities identified is examined by attempting to exploit the vulnerability with the aim of compromising the system.	
Expected results:	**Done**
• Extended list of the patch levels of systems and applications	☐
• List of actual vulnerabilities	☐
• List of the potential vulnerabilities which were unable to be verified using stealth techniques	☐
Requirements:	
Results of I 12: List of potential vulnerabilities	
Test steps:	**Effort**
• Use state-of-the-art vulnerability scanners (see A.7), but only perform scans which are difficult or impossible to detect. The number of scans performed from one IP address must be strictly limited or the time between scans varied, etc.	medium
• Manual verification of the remaining vulnerabilities, such as tests of buffer overflow exploits, etc.	high to very high
Risks:	
Systems could crash while exploiting vulnerabilities or their performance could be impaired. Attempts to exploit identified vulnerabilities could be detected.	

E 2. Overt Verification of Actual Vulnerabilities	
The actual threat potential of the vulnerabilities identified is examined by attempting to exploit the vulnerability with the aim of compromising the system.	
Expected results:	**Done**
• Extended list of the patch levels of systems and applications	☐
• List of actual vulnerabilities	☐
• List of the potential vulnerabilities which were unable to be verified using stealth techniques	☐
Requirements:	
Results of I 12: List of potential vulnerabilities	
Test steps:	**Effort**
• Use state-of-the-art vulnerability scanners (see A.7)	medium
• Manual verification of the remaining vulnerabilities, such as tests of buffer overflow exploits, etc.	high to very high
Risks:	
Systems could crash while exploiting vulnerabilities or their performance could be impaired.	

E 3. Verification of Actual Vulnerabilities in Application Interfaces	
The actual threat potential of the vulnerabilities identified in communications (interfaces), e.g. while accessing a database via a web server, are examined by attempting to exploit the vulnerability with the aim of compromising the system.	
Expected results:	**Done**
• Extended list of the patch levels of systems and applications	☐
• List of the actual vulnerability in the application interfaces	☐
Requirements:	
Results of I 12 and I 13: Detailed system descriptions and a list of application interfaces	
Test steps:	**Effort**
• Use state of the art vulnerability scanners (see A.7)	medium
• Manual verification of the remaining vulnerabilities, such as tests of buffer overflow exploits, etc.	high to very high
Risks:	
Systems could crash while exploiting vulnerabilities or their performance could be impaired. Attempts to exploit identified vulnerabilities could be detected.	

E 4. Covert Router Testing	
The identified routers are examined for vulnerabilities and for ways in which they can manipulated.	
Expected results:	**Done**
• Information on router ACLs	☐
• Information on router configuration	☐
• Administrative access to routers	☐
Requirements:	
Results of I 8: List containing detailed information on identified routers	
Test steps:	**Effort**
• Attempt to log into the router using standard passwords. Brute force attacks should not be attempted since these are easy to detect (e.g. by an IDS) and the test should be covert (stealth test).	medium
• Identify router ACLs using appropriate tools (firewalking). The tester should take care that the test is stretched over a long period of time in order to make it more difficult to identify the attack.	high
• Check the reaction of the router to fragmented and spoofed packets that can be created using a packet generator. The tester should take care that the test is stretched over a long period of time in order to make it more difficult to identify the attack.	very high
Risks:	
The attack could be detected. The performance of the router could be impaired.	

E 5. Overt Router Testing	
The identified routers are examined for vulnerabilities and for ways in which they can manipulated.	
Expected results:	**Done**
• Information on router ACLs	☐
• Information on router configuration	☐
• Administrative access to routers	☐
Requirements:	
Results of I 9: List containing detailed information on identified routers	
Test steps:	**Effort**
• Attempt to log into the router using standard passwords and brute force attacks	medium
• Identify the router ACLs using appropriate tools (firewalking)	very high
• Check the reaction of the router to fragmented and spoofed packets that can be created using a packet generator	very high
Risks:	
The performance of the router could be impaired.	

E 6. Test of Trust Relationships Between Systems	
The tester attempts to obtain unauthorized access through trust relationships between systems, e.g. by exploiting trusted hosts during user authentication.	
Expected results:	**Done**
• List of trust relationships between systems	☐
• Gleaning unauthorized information	☐
• Unauthorized access to files or systems	☐
Requirements:	
Results of I 6 and I 7: Descriptions of systems and applications	
Test steps:	**Effort**
• Analyze the information available in relation to potential dependencies and trust relationships between systems	high
• Attempt to obtain access using spoofing IP addresses or other authentication features	very high
Risks:	
The performance of the systems could be impaired.	

E 7. Covert Firewall Test From Outside	
The tester attempts to circumvent the firewall system, i.e. to create a network connection to the secured network segment from the outside. The tester can also attempt, for example, to gain control of the firewall system or exploit misconfigurations.	
Expected results:	**Done**
• List of firewall rules that can be inferred externally	☐
• Verification of the identified firewalls vulnerabilities	☐
• List of the systems that can be reached behind the firewall	☐
Requirements:	
Results of I 9: Information on the firewall components used	
Test steps:	**Effort**
• Identify firewall rules using appropriate tools (firewalking)	high
• Try to reach systems behind the firewall	very high
• Check the reaction of the firewall to fragmented and spoofed packets that can be created using a packet generator	very high
Risks:	
The performance of the firewall system could be impaired. The attack on the firewall could be detected by the firewall's log function, for example.	

E 8. Overt Firewall Test From Outside	
The tester attempts to circumvent the firewall system, i.e. to create a network connection from the outside to the protected network segment. The tester can attempt, for example, to gain control of the firewall system or exploit misconfigurations.	
Expected results:	**Done**
• List of firewall rules that can be inferred externally	☐
• Verification of the identified firewalls vulnerabilities	☐
• List of the systems that can be reached behind the firewall	☐
Requirements:	
Results of I 10: Information on the firewall components used	
Test steps:	**Effort**
• Run a vulnerability scanner on the firewall system hosts (firewall host, external router, internal router)	medium
• Identify firewall rules using appropriate tools (firewalking)	high
• Try to reach systems behind the firewall	very high
• Check the reaction of the firewall to fragmented and spoofed packets that can be created using a packet generator	very high
Risks:	
The performance of the firewall system could be impaired.	

E 9. Testing the Firewall From Both Sides	
Examination of the firewall by simultaneously testing both sides of the firewall. An externally placed system sends packets, an internally placed system analyzes the packets that arrive, and vice versa.	
Expected results:	**Done**
• List of firewall rules	☐
• Verification of the identified vulnerabilities of the type of firewall in use	☐
• Exhaustive list of the systems that can be reached behind the firewall	☐
Requirements:	
Results of I 10: Information on the firewall components used and network access to a point behind the firewall.	
Test steps:	**Effort**
• Test whether (possibly using tunneled protocols) unauthorized connections from the internal network to the internet can be created	high
• Run a vulnerability scanner on the firewall system hosts (firewall host, external router, internal router) from inside	medium
• Identify firewall rules using appropriate tools (firewalking from both sides)	high
• Check the reaction of the firewall to fragmented and spoofed packets that can be created using a packet generator	very high
Risks:	
The performance of the firewall system could be impaired.	

E 10. IDS System Testing	
This is a test of whether an existing IDS registers the potential attacks and sounds the alarm.	
Expected results:	**Done**
• IDS model	☐
• Reaction of the IDS to different types of attack	☐
• Statement on the performance of the IDS	☐
Requirements:	
Detailed information about systems and firewalls. Facility for monitoring whether the IDS system sounds the alarm.	
Test steps:	**Effort**
• Stage attacks that gradually become louder on the network of the target organization	low to very high
• Evaluate the reaction of the IDS to the attacks	very high
• Compare attack and IDS log files	high
Risks:	
These test steps can impair the performance of the target organization's network.	

E 11. Intercepting Passwords	
The tester attempts to intercept passwords by using interception tools (network sniffers, backdoors, etc.).	
Expected results:	**Done**
• Passwords in plain language	☐
Requirements:	
Appropriate system rights are needed to install interception tools. These can be obtained over a previously identified vulnerability. Data protection legislation must be observed.	
Test steps:	**Effort**
• Obtain rights for installing interception tools on appropriate systems	very high
• Install interception tools on appropriate systems	high
• Record and analyze network traffic on transferred passwords	high
Risks:	
The necessary installation of interception tools on appropriate systems can impair the performance of these systems. The necessary installation of interception tools on appropriate systems could make these systems accessible to non-authorized third persons.	

E 12. Password Cracking	
The tester uses different methods to attempt to find a password which allows privileged access to a system/application.	
Expected results:	**Done**
• Passwords in plain language	☐
Requirements:	
Password files that contain the encrypted passwords must be available for performing offline attacks, e.g. from E 11 or provided by the client. It must be possible to connect to the protected systems to perform online attacks.	
Test steps:	**Effort**
• Check the password files using appropriate tools (offline)	medium to very high
• Carry out online attacks if no password file is available for an offline attack	high
• Manual test of standard passwords or frequently used passwords	medium
Risks:	
User accounts could be locked if a maximum number of incorrect password entries has been defined in the application/operating system being tested.	

E 13. Test of Susceptibility to Denial of Service Attacks	
The tester examines the extent to which the system is susceptible to a denial of service attack.	
Expected results:	**Done**
• List of systems that are prone to DoS attacks	☐
Requirements:	
Systems susceptible to DoS attacks (web servers, mail servers, etc.) must be available.	
Test steps:	**Effort**
• Analyze the results of module I 12 Vulnerability Research	medium
• Carry out a DoS attack using various techniques	medium to very high
Risks:	
Even when the test reveals that the affected system is not susceptible to a DoS attack, a large-scale distributed DoS attack (DdoS), which would hardly be feasible for a tester, could still be successful. The performance of the tested system or involved network components could be impaired or may crash.	

E 14. Computer-Based Social Engineering	
The tester attempts to influence a person in order to obtain system rights by using appropriate computer-based manipulation techniques, e.g. by exploiting curiosity or helpfulness.	
Expected results:	**Done**
• Access to the organization's network or systems	☐
• List of system and application passwords	☐
Requirements:	
Results of I 6, I 7, I 13 – I 16: Information on target systems, applications and people	
Test steps:	**Effort**
• Contact the target person by e-mail	medium
• Trick target persons into installing special programs (e.g. keyloggers).	medium to high
• Ask target persons to enter user names and passwords using falsified system messages	medium to high
Risks:	
The attack could be recognized and cause the target person to worry. The special programs could disrupt operations.	

E 15. Direct, Personal Social Engineering With Physical Access	
The tester attempts to elicit confidential information by making direct contact with a person who has access to privileged information (e.g. by visiting him/her). The tester attempts to persuade the target person to reveal information by feigning a relationship of trust. The target person can be an employee of the organization or another insider.	
Expected results:	**Done**
• Relevant information such as passwords, system configurations, etc.	☐
Requirements:	
Results of I 7, I 14 – I 16: Information on target systems, applications and people	
Test steps:	**Effort**
• Make personal contact with the target person (e.g. pretending to be a service technician or new employee etc.)	medium
• Feign a relationship of trust to persuade the target person to surrender information (e.g. surrender a key or disclose passwords)	high
Risks:	
The attack could be recognized and cause the target person to worry. If the target person does surrender relevant information, this fact could impinge on the relationship between the target person and target organization once the penetration test is concluded and the person becomes aware of his/her misconduct, particularly when the said person is an employee of the target organization.	

E 16. Indirect, Personal Social Engineering Without Physical Access	
The tester attempts to find out secrets by contacting a person who is privy to privileged information by telephone. The tester attempts to persuade the target person to reveal information by feigning a relationship of trust. The target person can be an employee of the organization or another insider. The employee's naivety and his/her need to be involved and willingness to help is exploited.	
Expected results:	**Done**
• Relevant information such as passwords, system configurations, etc.	☐
Requirements:	
Results of I7, I14 - I16: Information on target systems, applications and people	
Test steps:	**Effort**
• Contact the target person by telephone or e-mail	medium
• Feign a relationship of trust to persuade the target person to surrender information (e.g. pretending to be an administrator, employee or distant superior, etc.)	high
Risks:	
The attack could be recognized and cause the target person to worry. If the person does surrender relevant information, this fact could impinge on the relationship between target person and target organization after the penetration test has been concluded and the said person is made aware of his/her misconduct (especially if he/she is an employee of the target organization).	

E 17. Wireless Communications Testing	
The tester attempts to obtain access to an existing WLAN.	
Expected results:	**Done**
• List of the vulnerabilities of the WLAN	☐
Requirements:	
Results of I 17: Information on an installed WLAN	
Test steps:	**Effort**
• Analyze the results of module I 17 Wireless Communications Testing (Scanning Only)	medium
• Exploit potential vulnerabilities	very high
• Attempt to connect to a WLAN	medium
• Attempt to obtain access to the WLAN	high
• Attempt to obtain access to data in the WLAN	very high
Risks:	
The penetration test could impair the performance of the WLAN.	

E 18. Testing Administrative Access to the Telephone System	
The tester attempts to obtain administrative access to the telephone system. External maintenance points of access not protected by a static call-back procedure and preset standard passwords and PINs, in particular, pose a high risk.	
Expected results:	**Done**
• Administrative access to the telephone system	☐
Requirements:	
Results of I 18: Information on the telephone system	
Test steps:	**Effort**
• Analyze the results of module I 18 Telephone System Testing (Identification)	high
• Attempt to obtain administrative access to the telephone system	very high
Risks:	
The test steps could impair the performance of the telephone system.	

E 19. Voicemail System Testing	
The tester attempts to circumvent the security functions of the mailbox system and gain access to mailboxes.	
Expected results:	**Done**
• Access to some mailboxes	☐
Requirements:	
Results of I 19: Information about the voice mail system	
Test steps:	**Effort**
• Analyze the results of module I 19 Voicemail System Testing (Identification)	medium
• Test whether access can be gained using preset passwords/codes	medium
• Carry out other technical tests that require specialist knowledge of the telephone system model in use	very high
Risks:	
The basic rights of affected mailbox owners could be impaired (privacy protection).	

E 20. Testing Administrative Points of Access to the Fax System	
The tester attempts to circumvent the security functions of the fax system and obtain administrative access to the fax system.	
Expected results:	**Done**
• Administrative access to fax system	☐
• Verification of vulnerabilities	☐
Requirements:	
Results of I 20: Information on the fax system	
Test steps:	**Effort**
• Analyze the results of module I 20 Fax System Testing (Identification)	medium
• Carry out other technical tests that require specialist knowledge of the fax system in use	very high
Risks:	
The test steps could impair the performance of the fax system.	

E 21. Modem Testing	
The tester attempts to obtain access to the network of the target organization using non-secure modems to circumvent the firewall.	
Expected results:	**Done**
• List of "wild" modems	☐
• List of the successful penetration attempts	☐
Requirements:	
Telephone number ranges or list of modem telephone numbers	
Test steps:	**Effort**
• Use a war dialer (with system detection components) on the target organization's number range	high
• Attempt to penetrate the network via the identified modem connections	very high
Risks:	
None	

E 22. Active Test of Access Controls	
The tester attempts to overcome access control mechanisms in order to obtain physical access to the buildings and rooms of the target organization.	
Expected results:	**Done**
• Obtaining access to protected areas	☐
Requirements:	
Results of I 22: Information on access controls	
Test steps:	**Effort**
• Analyze the results of module I 22 Access Control Identification	medium
• Test whether access to the site/building of the target organization is granted	medium
• Test whether it is possible to enter the site/building of the target organization unnoticed	medium
• Carry out additional tests of whether access can be obtained to the server systems or desktop computers	high
Risks:	
If discovered, the attempt to gain access could make employees feel worried and/or call the police.	

E 23. Test of Escalation Procedures	
The tester checks to extent to which escalation procedures are complied with in the event of an attack and how effective the procedures are.	
Expected results:	**Done**
• Assessment of the proper functioning of the established escalation procedures in practice	☐
Requirements:	
Means of monitoring the reactions of the client's employees to the attempted attacks	
Test steps:	**Effort**
• Progressively "louder" types of attacks are performed on the network of the target organization in order to activate escalation procedures	low to very high
• The reports of the attacks performed are compared with the countermeasures introduced.The appropriateness of the countermeasures is assessed.	medium
Risks:	
These test steps can impair the performance of the target organization's network.	

6.6 Penetration Test Documentation

The scope and content of the documentation the tester delivers to the client at the end of testing must be set out in the contract. The following may be included in a complete set of documents:

- the contract, including the results and agreements negotiated in the preparatory talks (see 4.3),
- documentation of the test steps completed for reconnaissance, e.g. using form A.6.1, the log files of the tools used, including the list of vulnerabilities tested,
- the system descriptions derived from these (see form A.6.3),
- a list of potential vulnerabilities, broken down according to system with a brief description,
- the results of the risk analysis (time/cost and priorities) and the systems or E modules selected on this basis for phase 4 (active intrusion attempts),
- documentation of the modules completed for active intrusion attempts, e.g. using form A.6.2 and the log files of the tools used,
- the individual results of the E modules including the list of verified vulnerabilities, and
- a final report.

If high demands are placed on the transparency of the penetration tests, further documentation may be required. Here, keyboard and mouse recorders as well as monitor or terminal logging utilities and/or network monitors/sniffers may be used.

The individual parts of the documentation may contain highly sensitive information, such as passwords or open vulnerabilities. The entire documentation must therefore be treated confidentially. Moreover, the parties must agree to who from the client's organization receives which parts of the documentation. Certain parts, e.g. personal data, should be delivered to the the data protection officer only, and not to the IT department.

7 Performing Penetration Tests

This chapter describes, with examples, how penetration tests are conducted applying the methodology presented above. The steps contained in phases 1 to 5 are explained in detail, with potential problems being highlighted. This chapter also describes what documentation has to be prepared at which stage.

7.1 Preparation

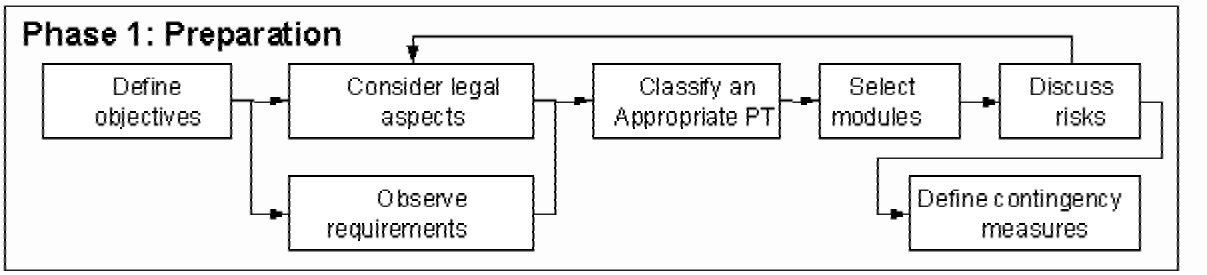


Figure 4 : Phase 1 – preparing the penetration test:

The preparation phase starts with defining the goal or goals of the penetration test. The tester and the client should jointly define goals so that both parties share the same understanding of the objectives. Possible goals of penetration testing are to improve the security of the technical systems, have IT security confirmed by an external third party, and increase the security of the organizational/personnel infrastructure (cf. Section 3.2).

In accordance with these objectives, the legalities of the penetration test (cf. Section 5.3) and the organizational, personnel and technical requirements (cf. Sections 4.2, 5.1 and 5.2) will have to be observed and discussed by client and tester.

With the aid of the classification (cf. Section 3.4), an appropriate test is then selected using the six criteria of information base, aggressiveness, scope, approach, technique and starting point.

If a penetration test is being carried out for the first time the test should ideally cover all existing systems as vulnerabilities could remain in the systems that are not investigated.

The amount of time to be spent on testing should ideally be estimated on the basis of the results of a prior assessment of protection requirements, applying, for example the methodology of the Baseline Protection Manual ("*Grundschutzhandbuch*"). [BSI02]

On the basis of the chosen classification, the tester selects the reconnaissance and active intrusion attempt modules to be conducted by excluding the modules that can be left out (cf. 6.4.1).

The risks for the client vary depending on the modules selected, and can range, for example, from postponing maintenance work (low risk) to the permanent failure of an IT system (high risk). The client and tester must discuss the likelihood that such risks will occur and their potential effects. As a

result of the discussion the parties should define the necessary contingency measures for the risks which both parties are willing to take. When defining the contingency measures, the parties should consider the time frame within which critical tests can be carried out and who will be responsible for the necessary measures. If the choice of modules involves unacceptable risks, a different penetration test will have to be chosen, e.g. a less aggressive approach for active intrusion attempts, abandoning social engineering techniques, or a reduced scope of the systems to be tested. If need be, the organizational and legal framework will have to be considered or discussed again at this stage.

All the results of the preparation phase should be recorded in writing in a report and signed by both parties. The client can use this report to monitor the penetration tests, for example, and it can serve as a guideline for the tester.

In addition, the extent of the documentation to be delivered after completion of the penetration test should be defined in the contract. The purpose of the documentation should be to allow the penetration testing process to be traced. A note on techniques for documenting penetration tests can be found in Section 6.6 , Appendix A.5.1 contains appropriate documentation forms.

The preparation phase must culminate in a detailed plan stating precisely when which components are penetrated with which level of intensity. Escalation stages also need to be defined, i.e. contingency measures have to be devised for sensitive systems, such as data backups, alternative systems and which service providers will need to be available.

The test times should be defined roughly, at least for business-critical systems, to avoid disrupting the client's operations, for instance. Another decision which may need to be made is which members of the functional departments will have to be informed about the test.

Classifying data helps to define the intensity and approach for the tests (production servers are tested differently to test servers). If, for example, a cluster has to be tested, the parties will have to decide whether an audit would not be better for identifying vulnerabilities. In the case of self-developments, the support employees concerned should be involved in deciding which precautions are necessary and feasible.

Finally, before the test is launched it should be clear how the results of the penetration test will be treated. A positive and constructive approach is helpful if the recommendations are to be translated into action to improve IT security infrastructure.

7.2 Reconnaissance

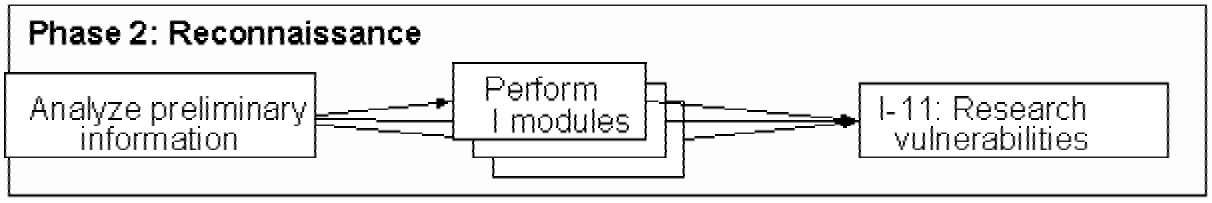


Figure 5 : Phase 2 – reconnaissance

Phase 2: Reconnaissance starts with an analysis of the preliminary information. In a black-box test, the preliminary information may be no more than an IP address or IP address block. If detailed information has been made available in a white-box test (such as operating system versions, applications used, etc.), the tester should start by analyzing this information and, if need be, request more information, such as system descriptions, network plans, etc. from the client to ensure that the test is carried out as efficiently as possible.

In the next step, the test procedures of the selected I modules are conducted. The tester is more or less free to choose the order in which the modules are completed. Only module I 12: "Vulnerability Research" has to be carried out after the preceding I modules because it uses the results of those modules, for example the list of available systems and program versions. The information gleaned is used in I 12 to identify the vulnerabilities in the systems and applications, with public and private databases being queried for known weak points and security loopholes. This procedure is illustrated by the following example:

The tester has identified a server in the client's DMZ, a potential target for the penetration test, as an e-mail server and has found out the version of the e-mail server software and the server's operating system using a banner lookup. With this information, the tester looks for potential vulnerabilities associated with this combination in databases, mailing lists and newsgroups, etc. Vulnerability scanners can carry out some of these testing steps automatically, however, with unusual combinations they often come up against limiting factors and fail to report or overlook existing vulnerabilities. They are therefore no substitute for a manual search, but they can supplement and accelerate the process.

At the end of the reconnaissance phase the tester will have the log files of the I modules that are generated by vulnerability scanners, for instance, a description of the systems, and a list of potential vulnerabilities, all of which should be included in the penetration test documentation.

7.3 Analysis of Information / Risks

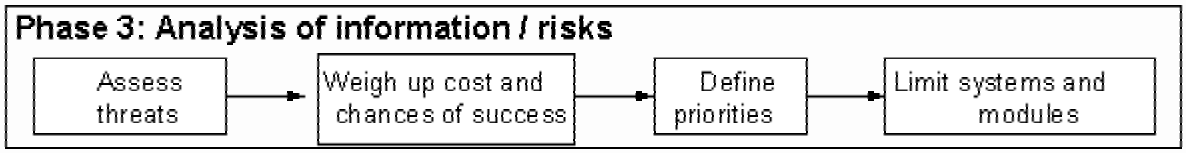


Figure 6 : Phase 3 – analysis of information and risks

The first step should be to assess the risks involved. Given the wealth of information that is usually obtained, it is important to analyze and evaluate this information before going any further. The evaluation has to include the defined goals, potential threats to the systems and the estimated cost of evaluating security flaws. Vulnerabilities can be assessed objectively and the risk potential can be established using the SANS Security Alert Consensus (SANS-SAC), for example, which is updated on a weekly basis. The evaluation will always be subjective because the tester's experience and specialization, for instance, play a major role in estimating time and cost.

Once the threat has been assessed, the tester should estimate the individual cost of a successful attack that exploits the potential vulnerabilities and weigh it up against its chances of success. A rough time schedule for the testing steps can be derived from the times stated in the module descriptions (time required: medium, high, very high). Priorities should then be defined on the basis of this comparison. The greater the likelihood of success and the lower the time/cost required, the higher the priority should be. The tester should document both the time/cost estimate and the priorities he sets.

Based on the tester's priorities, the targets and testing steps for the next stage, phase 4, can be chosen. The next testing steps should focus primarily on the IT systems which, after the evaluation of potential vulnerabilities, have been assessed as being high to medium priority, and on those test procedures that are most likely to be successful. For this, the selected E modules are limited further (cf. 6.5.2). A written shortlist of systems and modules should be attached to the penetration test documentation and be discussed with the client prior to any active intrusion attempts.

7.4 Active Intrusion Attempts

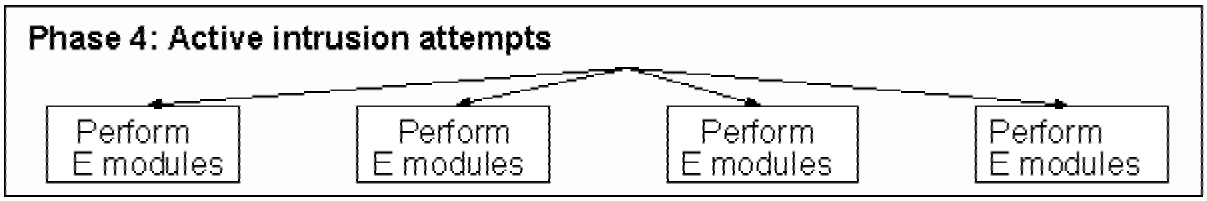


Figure 7 : Phase 4 – carry out active intrusion attempts

Once the relevant E modules have been selected and prioritized, in this stage the IT systems are actively assailed. The tester systematically works through the attack attempts in order of their priority, the highest priority first.

The client's targets for penetration testing are usually particularly business-critical systems, so special care is called for in carrying out intrusion attempts. The contingency measures mentioned in the preparation phase are absolutely essential in this stage. They demand, for example, that intrusion attempts (on business-critical systems) be made outside working hours (i.e. at night or weekends) and that the responsible system administrators be present.

The process is illustrated below taking module E 3 "Verification of actual vulnerabilities in application interfaces" as an example.

In the reconnaissance phase a specific server operating system with a web server application was identified on a system that is used for online transactions and which accesses the company's internal ERP system. The vulnerability search revealed a buffer overflow vulnerability for the underlying database in the ERP system. However, the firewall prevents direct access to the database. The tester now faces the challenge of finding out whether an online transaction that penetrates the firewall to exploit the vulnerability in the database system can be triggered by manipulating an HTTP link.

Not until active penetration attempts are carried out does it become clear whether the potential vulnerabilities identified in the reconnaissance phase can actually be exploited so that the selected system can be penetrated, for example. If the client asks for the potential vulnerabilities to be listed and also tested, both tester and client should carefully weigh up the possible consequences (e.g. system downtime).

The documentation should detail both positive, i.e. successful active intrusion attempts, and negative results, i.e. unsuccessful penetration attempts.

7.5 Final Analysis / Clean-Up

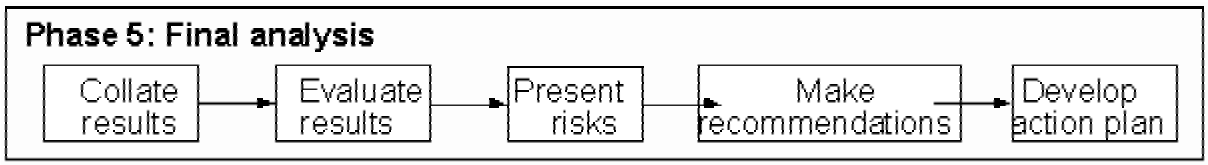


Figure 8 : Phase 5 – final analysis and clean-up

In this final phase the results of each of the E modules that were carried out are compiled in a final report. The final report should comprise a management summary describing the test engagement, key test results, and recommended action on an abstract level and is designed for top management. The main section of the final report should contain the detailed positive and negative test findings, as agreed. For the vulnerabilities, the results are evaluated and prioritized, and the tester describes the

ensuing risks so that the client knows which risks are relevant to his business operations. In addition, the report should contain recommendations on how the client can eliminate the vulnerabilities existing at the time of the penetration test. The final report should also include an action plan for eliminating vulnerabilities, based on the priorities assigned to the results and drawn up together with the client. The action plan should contain a schedule for each critical vulnerability and name a person and/or area that is responsible for its elimination.

The sensitive personal data obtained during penetration testing (cf. Section 6.6), such as passwords or private e-mails should not be included in the final report for data protection reasons; they should be handed over to a designated person, e.g. the data protection offer. However, the client must be able to trace the test results clearly, and all information gathered in the various phases must be included, at least as an appendix to the working papers. This includes, for instance, detailed information on the tools used, work steps (which tool was used with which options), log files, work times (when were attacks carried out), etc.

The tester has to remove any software, such as keyloggers, that may have been installed in the client's IT system in the course of the penetration test or any other modifications made to the client's IT systems, and restore the system to the state in which the tester found it prior to testing.

Glossary

Term	*Explanation*
Back door	A computer program that establishes undocumented or secret access to the computer via the network.
Black-box test	A penetration test in which the tester has no prior information about the network he/she is testing.
Browser	A program for presenting websites on the internet or intranet.
CERT	Computer Emergency Response Team; a group of IT specialists who ward off attacks on IT systems.
CGI	Common Gateway Interface; program for processing data on a web server that has been transferred from a ➔ browser.
Cracker	A person who obtains unauthorized access to or manipulates other IT systems, often with unlawful intentions.
DDoS	Distributed ➔ Denial-of-Service; a DoS attack in which the target system is attacked by means of simultaneous attacks on a number of distributed systems.
Denial-of-Service (DoS)	A cracker's attacking method in which he tries to impair the availability of an IT system by overloading it.
DMZ	De-Militarized Zone; a decoupled, isolated partial network located logically between an insecure network and a network that has to be protected and normally contains servers or services such as web servers and e-mail servers that can be accessed externally.
DNS	➔ Domain Name System
Domain Name System	A mechanism for turning computer names into ➔ IP addresses.
DoS	➔ Denial-of-Service
Escalation procedures	Instructions on how to respond to a hacker attack.
Filter rules	Information for controlling a ➔ firewall.
Firewall	Protection measure between two computers when one has a higher

Term	*Explanation*
	protection requirement.
FTP	File Transfer Protocol; application layer protocol for the transfer of files.
GoBS	Generally Accepted Accounting Principles of Computer-Assisted Accounting Systems (*Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme)*; minimum requirements on the functionality and control of data-processing systems derived from the German Commercial Code.
Hacker	A person with a technical interest in the functionality of hardware and software and therefore has the know-how necessary for circumventing security arrangements in hardware and software. Often no distinction is made between a hacker and a ➔ cracker in everyday language, while the distinction is normally upheld in specialist circles.
Host	Operator of a server.
HTTP	Hypertext Transfer Protocol; application layer protocol for presenting websites.
IDS	➔ Intrusion Detection System
ICS	➔ Internal Control System
Internal Control System	All measures that serve to minimize an organization's risks, avert damage and secure its assets.
Internet Service Provider	➔ Provider
Intrusion Detection System	Security software that detects network-based attacks and, if necessary, responds to them.
IP address	A number that consists of four blocks of numbers between 0 and 255 (written in decimals) and which can be used address a system on the internet or intranet.
ISP	➔ Internet Service Provider
LAN	Local Area Network.
Linux	A free (➔ Open Source) Unix compatible operating system.
News groups	News and discussion forums on the internet.
Open Source	An initiative that promotes the free availability of software and the

Term	*Explanation*
	disclosure of the corresponding source codes.
OSI reference model	Seven-layer model for demonstrating and standardizing communication between computer systems.
Outsourcing	Purchase of services (previously rendered in-house) from third parties.
P2P Client	Peer-To-Peer Client; a computer program for exchanging or downloading all manner of files.
Packet filter	Security layers 1 to 3 of the ➔OSI reference model.
Provider	Service provider, mostly offering access to the internet. A ➔host is also a provider in this sense.
Router	A network device that connects two or more networks.
Vulnerability scanner	Security software which allows systems to be checked for potential software vulnerability and security gaps.
Security policy	A document that describes the security objectives of an organization in an abstract way.
SMTP	Simple Mail Transfer Protocol; an application layer protocol mainly used for transferring e-mails.
Sniffer	A tool for intercepting network traffic.
Social engineering	An attacking method that entails tricking people to disclose sensitive information (e.g. passwords) or otherwise manipulating them.
Spoofing	The attacking method of a cracker who attempts to deceive systems or persons through technical manipulation (e.g. faking a false IP address, faking a false DNS address etc.).
TCP/IP	A network protocol used on the internet and in internal networks.
Tiger team	A group of penetration testers.
Trojan horse	A program that performs harmful functions in the background that go unnoticed by the user (e.g. intercepting and transferring passwords).
WAN	Wide Area Network; an organization-wide network that spans several different sites.
War dialer	A hacker tool that dials blocks of telephone numbers automatically and elicits information from the machine that answers. Often used for

Term	*Explanation*
	localizing unsecured modems.
War walking	To establish the existence and spread of WLAN networks.
War driving	➔ War walking from a vehicle.
Web bug	An invisible part of a website which enables a system not visible to the user to intercept information on the user's system configuration (IP address, browser version etc.).
Web server	A computer that makes information available on the internet for retrieval.
Web hosting	Operation of a ➔ web server on behalf of a customer.
White-box test	A penetration test in which the tester has prior information on the network he/she is testing.
WLAN	Wireless Local Area Network.

Bibliography

[Andersen99].	Arthur Andersen, KontraG – Erläuterungen zu den wichtigsten Vorschriften und praktische Hinweise zur Umsetzung, 3rd edition 1999
[Anonymous01]	Anonymous: Der neue Hacker's Guide, 2nd edition, Markt & Technik 2001
[BSI02]	IT Baseline Protection Manual (*Das IT-Grundschutzhandbuch*), May 2002, Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de/gshb/index.htm
[BSI01]	Die BSI Firewallstudie II, 2001, http://www.bsi.de/literat/studien/firewall/fwstud.htm
[CCC02]	Chaos Computer Club, http://www.ccc.de/congress/2001/overview.de.html
[CSEG02]	CSEG Communications-Electronic Security Group, http://www.cseg.gov.uk/partnerships/pwi/check/index.htm
[CSI02]	CSI Computer Security Institute, 2002 CSI/FBI Computer Crime and Security Survey, http://www.gocsi.com
[Discovery02]	Discovery.com, http://www.discovery.com/area/technology/hackers/crunch.html
[Emmert02]	Emmert, Ulrich: Strafbare Sicherheits-Tools?, in KES Zeitschrift für Kommunikations- und EDV-Sicherheit, Vol. 2, Year 18. 2002, p.6-9
[Fuhrberg01]	Fuhrberg/Häger/Wolf: Internet-Sicherheit, 3rd edition., Hanser 2001
[GIAC02]	GIAC, 2002, http://www.giac.org
[Herzog02]	Herzog, Pete: Open Source Security Testing Manual OSSTMM, 2002, http://www.osstmm.org/
[ISACA02]	Information Systems Audit and Control Association, 2002, http://www.isaca.org/
[ISACA_CH99]	ISACA Switzerland: Sicherheitsüberprüfung von IT-Systemen mit Hilfe von Tiger Teams, 1999, http://www.isaca.ch
[ISC02]	International Information Systems Security Certifications Consortium, 2002, http://www.isc2.org/
[Kabay00]	Kabay, Michel E.: Social engineering simulations, Network World Security Newsletter, Dec. 18, 2000, http://www.nwfusion.com/newsletters/sec/2000/00292157.html

[Klevinsky02]	Klevinsky/Laliberte/Gupta: Hack I.T. – a guide to security through penetration testing, 1st edition, Addison Wesley 2002
[Kurtz02]	Kurtz/McClure/Scambray: Das Anti-Hacker Buch, 3rd edition, MITP 2002
[LfDN99]	Landesbeauftragter für den Datenschutz Niedersachsen, Grundschutz durch Firewalls, 1999, http://www.lfd.niedersachsen.de
[LfV98]	Landesamt für Verfassungsschutz Baden-Württemberg: Wirtschaftsspionage – die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste, 1998
[NIST02]	NIST Guideline on Network Security Testing, http://csrc.nist.gov
[SANS]	SANS Institute, http://www.sans.org
[SANS-SAC]	SANS Security Alert Consensus http://www.sans.org/newlook/digests/SAC.htm
[Schneier01]	Schneier, Bruce: Secrets & Lies – IT-Sicherheit in einer vernetzten Welt, 1st edition, Wiley 2001
[Sptimes01]	St. Petersburg Times: A history of hacking, http://www.sptimes.com/hackers/history.hacking.html, 2001
[TLC02]	TLC, http://tlc.discovery.com/convergence/hackers/articles/history_03_print.html
[Venema95]	Venema, Wietse: SATAN Security Administrator Tool for Analyzing Networks, http://www.fish.com/satan/
[Vosseberg01]	Vosseberg, Thomas: Hackerz Book, 1st edition, Franzis 2001

Appendix

A.1 OSSTMM

The Open Source Security Methodology Manual (OSSTMM) [Herzog02] is a relatively well known guideline on penetration testing methodology. The OSSTMM is the result of an initiative launched by Pete Herzog. This work is an open source project that lists the steps that have to be performed in a penetration test. Several authors constantly work on improving this model and make it available to the public. At the time of writing, the latest release of the OSSTMM is version 6.0 RC. The aim of the OSSTMM is to set quality standards for penetration testing. The OSSTMM is aimed at IT security service providers who, if they perform penetration tests in accordance with the OSSTMM model, are authorized to display the OSSTMM logo on their test reports.

The OSSTMM divides the area investigated in a penetration test into six sections: internet security, information security, physical security, communications security, wireless security, and social engineering. Each section has its own modules dealing with the relevant test areas. Each of these modules is explained briefly and the anticipated results are listed. The modules consist of tasks to be completed by carrying out the individual testing steps. The OSSTMM also contains several templates for documenting the results of the testing steps in the various modules.

There are two different approaches that can be taken in using the OSSTMM: either the modules are completed successively one after the other, or, alternatively, independent modules are carried out simultaneously.

The OSSTMM suggests a system of RAVs (risk assessment values) to measure how often modules should be repeated. For each module there is pair of values, consisting of the “RAV cycle” and the “RAV degradation”. The RAV cycle value states the cycle (in days) in which the test should be repeated. The RAV degradation value denotes, as a percentage, how much security deteriorates within this cycle, on the assumption that the original test was performed with due care by an experienced tester. The quotient of the pair of values is used in the calculation, i.e. each of the two values influences the other and could be replaced by a single value.

This system was only introduced in the latest version (Version 2.0) of the OSSTMM and is therefore likely to be modified further in the open source process. What is more, RAVs are not at all indicative of absolute security; they merely describe a reduction in security over time in relation to the level immediately after testing.

The OSSTMM model does not address the objectives of penetration testing. It is a kind of generic work program that can be adapted to meet individual requirements.

Modules or testing steps are not ranked in order of their priority. This means that tests that detect widespread vulnerabilities are not performed with higher priority than other steps that could have only very limited chances of succeeding in penetrating a system.

A.2 NIST Guideline on Network Security Testing

Another penetration testing model worth mentioning is the "Guideline on Network Security Testing" by the National Institute of Standards and Technology (NIST) [NIST02]. At the time of writing, the document was still in the drafting stage.

The Guideline describes a methodology for testing network security and is aimed at organizations wishing to investigate their own IT infrastructure by self-assessment. The task of network security testing is assigned a place in a system's life cycle. In addition, selected methods for testing network security are presented. The Guideline does not call all the methods in their entirety "penetration testing"; this term is reserved for one of many techniques (others include networking mapping or password cracking). The penetration testing technique is broken down into the successive phases of planning, discovery, attack and the parallel reporting phase.

A.3 ISACA Switzerland – Testing IT Systems Security With Tiger Teams

The Special Interest Group on Information Security of the Swiss Informaticians Society and the ISACA (Information Systems Audit and Control Association) Switzerland jointly published a pamphlet entitled "*Sicherheitsüberprüfung von IT-Systemen mit Hilfe von Tiger Teams*" (Testing IT Systems Security with Tiger Teams). [ISACA_CH99] The term "tiger team" refers to a group of penetration testers. The pamphlet deals with penetration testing, splitting the process into four stages:

- Acquisition, proposal and contract
- Risk analysis
- Testing
- Report and presentation

The work is not a coherent methodology since the various chapters were written by sub-working groups.

The "acquisition, proposal and contract" chapter contains a detailed description of important issues that need to be clarified in a contract before carrying out a penetration test

The "risk analysis" section contains a method for identifying and assessing risks associated with the penetration test.

The "testing" chapter comprises the tasks to be completed in a penetration test. The following tasks are covered:

1. **Carrier scan:** scan for modems than be accessed from outside.
2. **Internet scan:** scan for computer systems that can be accessed over the internet and their identification.
3. **Password cracking:** testing passwords and password policies.
4. **Manual hacking:** attempt to exploit the potential vulnerabilities identified in tasks 1 – 3.
5. **Intranet scan:** similar to 2, except over the internal network.
6. **System scan:** system analysis to identify general configuration and unnecessary services.
7. **Phreaking:** testing systems connected with the telephone system.
8. **Analysis of relationships of trust:** relationships of trust with business partners, customers and suppliers.

The "reporting" chapter explains the elements required for informative documentation and presentation of results.

The "risk analysis" chapter contains an interesting method for prioritizing and selecting test procedures to be carried out during the penetration test. An "overall risk" is identified in two steps and acts as a basis for deciding which techniques to employ. The steps are:

- Analysis of system risk

  Evaluates how prone the system concerned is to hacker attacks, applying the criteria of "threat" (how great is the potential threat to the system?), "hacker skills" (how skilled must a hacker be to exploit the risk?) and "internal/external" (is the threat from the inside and/or the outside relevant?).

- Analysis of risk of hacker attacks

  Evaluates the time required for an attack and the probability that an appropriate attack technique will succeed, together with a risk assessment of the effects of the attack. The outcome is a definite decision for or against the use of the technique. Available criteria are "chance of success" (how probable is it that the attack will be successful?), "effort required" (how time-consuming is the method of attack for the penetration tester?), and "risk assessment" (how serious are the potential effects of the attack on the system?).

Viewed as a whole, the work deals with issues such as risk analysis and efficiency of penetration testing. The chapters on contracts and reporting also contain quite detailed comments on the essential content of contracts and documentation.

Hacking techniques are described in the “testing" chapter. Efficiency is discussed at the beginning of the chapter, but the concept is not elaborated further in a method for choosing individual tasks.

A.4 Penetration Testing Certification

A.4.1 The CSEG CHECK Certificate

The CSEG (Communications-Electronics Security Group) is a British governmental authority that deals with aspects of IT security and provides advice to other authorities on issues of IT security. The CSEG has defined a standard for IT security service providers by introducing certification called CHECK (Computer IT Health Check Service). The CHECK initiative is designed to allow authorities and companies to identify qualified providers of IT security tests (IT Health Check) using the CHECK seal of quality [CSEG02].

In order to obtain CHECK certification, the IT security service provider must be a member of the CHECK service. The current annual membership fee is 7000 pounds Sterling. Membership includes participation in a one-day “CHECK Service Assault Course” that provides training in hacking methods and a final exam. If the participant passes the exam, he/she and his/her company are authorized to perform IT health checks in accordance with the CHECK model. The CHECK seal of quality is essential for contracts in the public sector and is used for promotional purposes in the private sector.

In order to be accepted into the CHECK service program, the following information must be disclosed to the CESG:

- details on the business structure of the IT security service provider
- details of the methodical approach for services
- the number of projects carried out in the last 12 months
- an (anonymized) copy of a report on an IT health check project detailing the subject of the contract, test findings and results
- details of contact partners for reference purposes
- details of any other certifications (ISO 9000)

- employee details: name, date of birth, nationality and curriculum vitae of all employees capable of performing IT health checks

To date, the CHECK certificate is fairly well received in Britain. One point of criticism is that only one employee of an IT security service provider needs to pass the exam to obtain for his/her organization the status of a CHECK-certified IT service provider.

A.4.2 The ISC² CISSP Certificate

The CISSP (Certified Internet Security Systems Professional) certificate is issued by the International Information Systems Security Certification Consortium (ISC²) [ISC02]. It is an exam that entitles the successful candidate to bear the CISSP title.

The ISC² was founded by a group of IT security service providers in 1988. The main objective of the ISC² is to establish standards in the field of IT security. These standards are referred to as CBKs (Common Body of Knowledge) and comprise a collection of information on the topic of IT security.

The objective of the CISSP initiative is to create certificates which IT security consultants can use as evidence of their expertise. The CISSP program has been in existence since 1992.

The exam covers the following areas:

- Access protection mechanisms and methods
- Application and system development
- Contingency planning
- Cryptology
- Legal background, forensic methods and ethics
- Security in current operations
- Physical security
- Security architectures and models
- Security management
- Telecommunications, network and internet security

In addition to passing the exam, there are further conditions that must be fulfilled before becoming certified. For example, the CISSP applicant must provide evidence of three years of professional

experience in the field of IT security and a reference either from another certified CISSP or from his employer. He/she must also follow the ethical codex of the ISC² and pay regular fees to the ISC².

The CISSP exam is relatively unknown in Germany. This is probably because the ISC² is not represented in Germany yet. The CISSP certificate is widely recognized in the USA. As yet, the ISC² has not published the exact number of CISSPs certified so far.

The ISC² has recently also started to offer the SSCP (System Security Certified Practitioner) exam. This certificate differs from the CISSP in that it caters to a target group of network administrators, while the CISSP certificate addresses a target group of security consultants/officers. The SSCP exam covers the following areas:

- Access protection mechanisms
- Administration
- Monitoring
- Risk, escalation procedures and startup processes
- Cryptology
- Data communication
- Malignant program codes/malware

We are currently unable to comment on the spread of the SSCP certificate or the extent to which it is recognized.

A.4.3 The SANS Institute GIAC Certificate

The SANS (System Administration, Networking and Security) Institute is a renowned organization that has made a name for itself through a number of publications in the field of IT security. Founded in 1989, the SANS Institute publishes, for example, the annual "SANS Top Twenty", a list of the 20 most widespread vulnerabilities of IT systems. [SANS]

The GIAC certification (Global Information Assurance Certification) has been in existence since 1999 with the aim of allowing consultants to provide evidence of their expertise.

The GIAC program consists of a series of individual exams and differs, according to the SANS Institute, from other certificates, in that it tests both theoretical knowledge and its practical application. In addition, the GIAC exams also cover advanced technical areas.

The objective of the certification is to obtain GSE status (GIAC Security Engineer) by passing a series of six exams. The GSE applicant must also write an essay on a topic relating to IT security which is then published on the SANS Institute homepage.

As well as the exams required for the GSE, there are further additional GIAC exams in other areas of IT security. The GSE exams are as follows:

- GSEC (GIAC Security Essentials)
- GCFW (GIAC Certified Firewall Analyst)
- GCIA (GIAC Certified Intrusion Analyst)
- GCIH (GIAC Certified Incident Handler)
- GCNT (GIAC Certified Windows Security Administrator)
- GCUX (GIAC Certified Unix Security Administrator)

According to the GIAC homepage, 3600 persons were certified in accordance with GIAC when this study was being compiled.

A.4.4 The ISACA CISA Certificate

The Information Systems Audit and Control Association (ISACA) is the world association of EDP auditors and awards the CISA (Certified Information Systems Auditor) Certificate. The ISACA was founded in 1968 and now numbers 17,000 members in 101 countries.

The objective of the CISA program is to create quality standards for IT auditors. In order to obtain the CISA title, the applicant must pass the CISA exam, have several years of professional experience in the area of IT audits and observe the ISACA's code of conduct .

The CISA exam contains questions from the following areas:

- IT management, planning and organization
- Technical infrastructure
- IT security
- Contingency planning
- System development, selection, introduction and maintenance
- Business process analysis and risk management

There are currently 23,000 people worldwide who bear the CISA title.

A.5 I and E Modules and Their OSSTMM Equivalents

The tables below show I and E modules and their equivalents in the OSSTMM 2.0 RC 6. [Herzog02] Since the OSSTMM does not differentiate between covert (stealthy) and overt (noisy) tests and because some OSSTMM modules have been combined, it is not possible to achieve a 1:1 or N:1/1:N match. Instead, they have to be matched N:M.

A.5.1 Reconnaissance Modules and Their Equivalents

No.	*Module*	*OSSTMM 2.0 RC 6*
I 1	**Analysis of Published Data**	M 2.03 Document Grinding
I 2	**Covert Queries of Basic Network Information**	M 1.01 Network Surveying
I 3	**Overt Queries of Basic Network Information**	M 1.01 Network Surveying
I 4	**Stealthy Port Scans**	M 1.02 Port Scanning
I 5	**Noisy Port Scans**	M 1.02 Port Scanning
I 6	**Application Identification**	M 1.03 Services Identification M 1.06 Internet Application Testing
I 7	**System Identification**	M 1.04 System Identification
I 8	**Covert Router Identification**	M 1.07 Router Testing
I 9	**Overt Router Identification**	M 1.07 Router Testing
I 10	**Covert Firewall Identification**	M 1.09 Firewall Testing
I 11	**Overt Firewall Identification**	M 1.09 Firewall Testing
I 12	**Vulnerability Research**	M 1.05 Vulnerability Research
I 13	**Application Interface Identification**	M 1.06 Internet Application Testing
I 14	**Collecting Information for Social Engineering**	M 3.01 Request Testing M 3.02 Guided Suggestion Testing M 3.03 Trusted Persons Testing
I 15	**Collecting Information for Computer-Based Social Engineering**	-
I 16	**Collecting Information for Personal Social Engineering**	M 3.01 Request Testing M 3.02 Guided Suggestion Testing M 3.03 Trusted Persons Testing
I 17	**Wireless Communications Testing (Scanning Only)**	M 4.01 Wireless Networks Testing M 4.02 Cordless Communications Testing M 4.04 Infrared Systems Testing
I 18	**Telephone System Testing (Identification)**	M 5.01 PBX Testing
I 19	**Voicemail System Testing (Identification)**	M 5.02 Voicemail Testing
I 20	**Fax System Testing (Identification)**	M 5.03 Fax Review
I 21	**Analysis of Physical Environment**	M 6.05 Location Review

No.	*Module*	*OSSTMM 2.0 RC 6*
I 22	**Access Control Identification**	M 6.01 Access Controls Testing M 6.03 Monitoring Review

A.5.2 Active Intrusion Modules and Their Equivalents

No.	*Module*	*OSSTMM 2.0 RC 6*
E 1	**Covert Verification of Actual Vulnerabilities**	M 1.05 Vulnerability Research
E 2	**Overt Verification of Actual Vulnerabilities**	M 1.05 Vulnerability Research
E 3	**Verification of Actual Vulnerabilities in Application Interfaces**	M 1.06 Internet Application Testing
E 4	**Covert Router Testing**	M 1.07 Router Testing
E 5	**Overt Router Testing**	M 1.07 Router Testing
E 6	**Test of Trust Relationships Between Systems**	M 1.08 Trusted Systems Testing
E 7	**Covert Firewall Test From Outside**	M 1.09 Firewall Testing
E 8	**Overt Firewall Test From Outside**	M 1.09 Firewall Testing
E 9	**Testing the Firewall From Both Sides**	M 1.09 Firewall Testing
E 10	**IDS System Testing**	M 1.10 IDS Testing
E 11	**Intercepting Passwords**	M 1.12 Password Cracking
E 12	**Password Cracking**	M 1.12 Password Cracking
E 13	**Test of Susceptibility to Denial of Service Attacks**	M 1.13 Denial of Service Testing
E 14	**Computer-Based Social Engineering**	-
E 15	**Direct, Personal Social Engineering With Physical Access**	M 3.01 Request Testing M 3.02 Guided Suggestion Testing M 3.03 Trusted Persons Testing
E 16	**Indirect, Personal Social Engineering Without Physical Access**	M 3.01 Request Testing M 3.02 Guided Suggestion Testing M 3.03 Trusted Persons Testing
E 17	**Wireless Communications Testing**	M 4.01 Wireless Networks Testing M 4.02 Cordless Communications Testing M 4.04 Infrared Systems Testing
E 18	**Testing Administrative Access to the Telephone System**	M 5.01 PBX Testing
E 19	**Voicemail System Testing**	M 5.02 Voicemail Testing
E 20	**Testing Administrative Points of Access to the Fax System**	M 5.03 Fax Review
E 21	**Modem Testing**	M 5.04 Modem Testing
E 22	**Active Test of Access Controls**	M 6.01 Access Controls Testing
E 23	**Test of Escalation Procedures**	M 6.03 Monitoring Review M 6.04 Alarm Response Review

A.6 Checklists and Documentation Forms

A.6.1 Checklist for Completing the I Modules

No.	*Module*	*Ref. no.*	*Done*
I 1	**Analysis of Published Data**		☐
I 2	**Covert Queries of Basic Network Information**		☐
I 3	**Overt Queries of Basic Network Information**		☐
I 4	**Stealthy Port Scans**		☐
I 5	**Noisy Port Scans**		☐
I 6	**Application Identification**		☐
I 7	**System Identification**		☐
I 8	**Covert Router Identification**		☐
I 9	**Overt Router Identification**		☐
I 10	**Covert Firewall Identification**		☐
I 11	**Overt Firewall Identification**		☐
I 12	**Vulnerability Research**		☐
I 13	**Application Interface Identification**		☐
I 14	**Collecting Information for Social Engineering**		☐
I 15	**Collecting Information for Computer-Based Social Engineering**		☐
I 16	**Collecting Information for Personal Social Engineering**		☐
I 17	**Wireless Communications Testing (Scanning Only)**		☐
I 18	**Telephone System Testing (Identification)**		☐
I 19	**Voicemail System Testing (Identification)**		☐
I 20	**Fax System Testing (Identification)**		☐
I 21	**Analysis of Physical Environment**		☐
I 22	**Access Control Identification**		☐

A.6.2 Checklist for Completing the E Modules

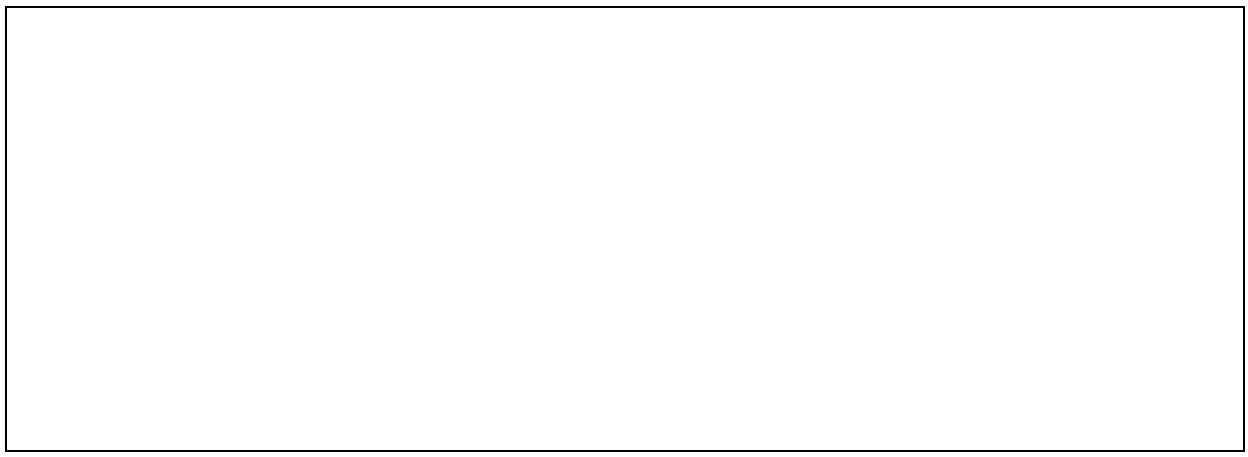
No.	*Module*	*Ref. no.*	*Done*
E 1	**Covert Verification of Actual Vulnerabilities**		☐
E 2	**Overt Verification of Actual Vulnerabilities**		☐
E 3	**Verification of Actual Vulnerabilities in Application Interfaces**		☐
E 4	**Covert Router Testing**		☐
E 5	**Overt Router Testing**		☐
E 6	**Test of Trust Relationships Between Systems**		☐
E 7	**Covert Firewall Test From Outside**		☐
E 8	**Overt Firewall Test From Outside**		☐
E 9	**Testing the Firewall From Both Sides**		☐
E 10	**IDS System Testing**		☐
E 11	**Intercepting Passwords**		☐
E 12	**Password Cracking**		☐
E 13	**Test of Susceptibility to Denial of Service Attacks**		☐
E 14	**Computer-Based Social Engineering**		☐
E 15	**Direct, Personal Social Engineering With Physical Access**		☐
E 16	**Indirect, Personal Social Engineering Without Physical Access**		☐
E 17	**Wireless Communications Testing**		☐
E 18	**Testing Administrative Access to the Telephone System**		☐
E 19	**Voicemail System Testing**		☐
E 20	**Testing Administrative Points of Access to the Fax System**		☐
E 21	**Modem Testing**		☐
E 22	**Active Test of Access Controls**		☐
E 23	**Test of Escalation Procedures**		☐

A.6.3 Form for Collecting Server Information

DNS name	
IP address	
Role	
Operating system	

Port	**Protocol**	**Application**	**Potential vulnerability**

Other information



A.6.4 Form for Collecting Social Engineering Information

Name	
Function	
E-mail	
Telephone	

Description of the attack	
Result	

A.6.5 Form for Collecting Further Information

Area/module	

Description of the test procedure	
Result	

A.7 Tools

The following table provides a list of hacker and security tools that can be used in penetration testing. Unless stated otherwise, the tools listed are freeware. The list does not compare the functionality of the tools and does not claim to be exhaustive.

Name	*Particularities*	*Platform*	*Source*
Port scanners			
7th Sphere Portscanner	Easy-to-use port scanner	Windows	http://www.computech.ch
Nmap	Port scanner with extended functions such as stealth scans or system recognition	Unix, Windows	http://www.insecure/nmap
Strobe	Fast TCP port scanner	Unix	ftp://suburbia.net/pub
Super Scan	Port scanner with an easy-to-operate user interface	Windows	http://www.computech.ch
Vulnerability scanners			
Cerberus Internet Scanner	Vulnerability scanner available either in a freeware version or a commercial version with extended functions.	WinNT, Win2000	http://www.cerberus-infosec.co.uk/cis.shtml
Happy Browse /THC	Vulnerability scanner that creates a list of potential vulnerable spots, but without any guidelines for exploitation	Windows	http://www.pimmel.com/thcfiles.php3
ISS Internet Scanner	Commercial vulnerability scanner	Win2000, WinXP	http://www.iss.net
Nessus	Vulnerability scanner made up of client and server components	Unix, Windows	http://www.nessus.org
Saint	Commercial vulnerability scanner	Unix	http://www.wwdsi.com
SARA	Freeware version of the commercial vulnerability scanner Saint	Unix	http://www-arc.com/sara
SATAN	First-generation vulnerability scanner, now obsolete and no longer updated	Unix	http://www.fish.com/satan
Xscan	Vulnerability scanner that can be operated from the instruction line and via a GUI.	Windows	http://www.xfocus.org/programs.php

Name	*Particularities*	*Platform*	*Source*
War dialers			
Phonesweep	Commercial war dialer, requires specialist knowledge	n.a.	http://sandstorm.net/products/phonesweep
THC Scan	Common war dialer for DOS/Windows	DOS	http://www.thehackerschoice.com
ToneLoc	Rather outdated war dialer	DOS	
CGI scanners			
Whisker	Tool for localizing security gaps in CGI scripts	Unix	http://sourceforge.net/projects/whisker
WLAN scanners			
Kismet	Tool for detecting and intercepting WLANs	Unix	http://www.kismetwireless.net
Net Stumbler	Tool for detecting WLANs	Windows	http://www.netstumbler.com
Other scanning tools			
Cheops	Supplies a graphical description of the scanned network	Unix	ftp://ftp.marko.net/pub/cheops
Firewalk	Tool for testing firewall rules	Unix	http://www.packetfactory
Languard	Port scanner with many additional functions	Win95, WinNT	http://www.gfi.com/downloads
Sam Spade	Universally implementable tool for obtaining information, incl. Whois and DNS queries	Windows	http://www.samspade.org
Visualroute	Supplies a graphical overview of traced routes	Unix, Windows	http://www.visualroute.com
What's running	Supplies information on software running on a target computer	Windows	http://www.woodstone.nu/whats
LAN sniffers			
Angst	Enables sniffing in switched networks	FreeBSD	http://wiretapped.net
Dsniff	Dnisff contains a collection of programs that allow the interception of network traffic in switched networks	Unix	http://www.monkey.org

Name	*Particularities*	*Platform*	*Source*
Ethereal	A packet sniffer that can also interpret application layer information	Windows, Unix	http://www.ethereal.com
Sniffit	Specially designed to record application data and passwords	Unix	http://reptile.rug.ac.be/~coder/sniffit/sniffit.html
Snort	Intrusion detection system with a sniffer component	Windows, Unix	http://www.snort.org
Tcpdump	Packet sniffer for OSI layers 1 to 4	Unix	http://www.tcpdump.org
Windump	Windows version of Tcpdump	Windows	http://winpcap.polito.it
WLAN sniffers			
AirSnort	This tool allows data recording in WLANS	Linux	http://sourceforge.net/projects/airsnort
WEPCrack	Can be used for cracking keys in WLANS	Linux	http://sourceforge.net/projects/wepcrack
Password crackers			
Brutus	Enables Telnet/FTP/Netbios/POP3 passwords to be cracked	Windows	http://hobbie.net/brutus/brutus-download.html
Crack	Allows Unix passwords to be cracked	Unix	http://www.users.dircon.co.uk/~crypto/
John the Ripper	Tool for cracking NT and Unix passwords	Unix, DOS, Windows	http://www.openwall.com/john
L0pht Crack	For cracking Windows passwords	Windows	http://www.atstake.com
Web Cracker	For overcoming web authentications	Windows	http://www.packetstormsecurity.org
Attacking tools			
Fragrouter	Tool for fragmenting packets	Unix	http://www.packetstormsecurity.com
Hping	For testing firewall rules, many other options	Unix	http://www.hping.org
Hunt	Tool for performing a session hijacking attack	Unix	http://www.wiretapped.net
IRPAS	Collection of programs	Unix	http://phenoelit.de
Jolt2	Tool for performing a DoS attack	Unix	http://www.securiteam.com/exploits/Jolt2_-_a_new_Windows_DoS_attack.html
Nemesis	Collection of tools for manipulating data packets	Unix	http://the.wiretapped.net

Name	*Particularities*	*Platform*	*Source*
RafaleX	Packet builder for manipulating IP/TCP/UDP packets	Windows	http://www.packx.net/packx
Stacheldraht	Tool for carrying out a distributed DoS attack (Ddos attack)	Unix	
TFN2000	Tool for carrying out a distributed DoS attack (Ddos attack)	Windows, Unix	
Trin00	Tool for carrying out a distributed DoS attack (Ddos attack)	Unix	
Trojan horses			
Back Orifice	Tools for remote operating a PC	Windows	http://www.cultdeadcow.com
Netbus	Tools for remote operating a PC	Windows	http://www.windowsecurity.com
Sub Seven	Tools for remote operating a PC	Windows	http://www.subseven.ws
Other tools			
Datapipe.c	Tool for rerouting connections and circumventing firewall rules	Unix	http://packetstormsecurity.nl/unix-exploits/tcp-exploits
Fpipe	Reroutes connections to another port and circumvents firewalls	Windows	http://www.networkingfiles.com
Netcat	Universally implementable tool for manipulating TCP and UDP connections	Windows, Unix	http://www.atstake.com