

## White Paper

# Performance and Possible Arrangements of Penetration Tests

Last Update: 09.09.2011

**SySS GmbH**  
<http://www.SySS.de>  
Wohlboldstraße 8  
72072 Tübingen  
Tel.: +49-7071-407856-0  
Fax: +49-7071-407856-19  
E-mail: [info@SySS.de](mailto:info@SySS.de)

### **Authors:**

Sebastian Schreiber    [Sebastian.Schreiber@SySS.de](mailto:Sebastian.Schreiber@SySS.de)  
Stefan Arbeiter        [Stefan.Arbeiter@SySS.de](mailto:Stefan.Arbeiter@SySS.de)

### **Quality Assurance:**

Micha Borrmann (Module LAN/WAN)    [Micha.Borrmann@SySS.de](mailto:Micha.Borrmann@SySS.de)  
Christoph Bott (Module WLAN)        [Christoph.Bott@SySS.de](mailto:Christoph.Bott@SySS.de)  
Katrin Heinrich (Module WebApp)      [Katrin.Heinrich@SySS.de](mailto:Katrin.Heinrich@SySS.de)



Sebastian Schreiber

#### **About the Managing Director**

- 1993 – 1999 studies of Information Technology, Physics, Mathematics and Business Studies at the Eberhard Karls University of Tübingen
- 1996 – 1998 Member of staff at Hewlett-Packard's
- 1996 MicroGold (USA)
- 1998 – today Managing Director of the SySS GmbH (Security tests at a vast number of different companies)
- Numerous publications, lectures in Germany and abroad; Co-Editor of the journal "IT-Sicherheit und Datenschutz" (IT Security and Data Protection)

# Contents

|   |    |
|---|----|
| 1. Summary .....  | 3  |
| 2. Possible Arrangements .....  | 3  |
| 2.1. Object to be Tested and Test Coverage .....                                      | 4  |
| 2.2. Test Depth .....   | 5  |
| 2.3. Test Frequency .....   | 5  |
| 2.4. Expertise of Security Testing .....  | 6  |
| 2.5. Test Perspective .....   | 7  |
| 2.6. Aggressiveness of Tests .....  | 8  |
| 2.7. Risks When Performing Security Tests .....                                       | 9  |
| 2.8. Announced and Unannounced Checks .....   | 11 |
| 2.9. Social Engineering .....   | 12 |
| 2.10. Hidden or Open Tests .....  | 12 |
| 3. Project Modules .....  | 13 |
| 3.1. Kick-Off: KICKOFF .....  | 13 |
| 3.2. Perimeter Detection: PERIM .....   | 14 |
| 3.3. Analysis from the Internet: INTERNET .....                                       | 15 |
| 3.4. Check of Web Applications: WEBAPP .....  | 18 |
| 3.5. Security Test in the Internal Network: LAN/WAN .....                             | 27 |
| 3.6. WLAN Test: WLAN .....  | 31 |
| 3.7. Product/Laboratory Tests: PRODUCT .....  | 34 |
| 3.8. Documentation: DOCU .....  | 36 |
| 3.9. Presentation Workshop: PRES .....  | 37 |
| 3.10. Additional Test: RETEST .....   | 38 |
| 4. Special Examinations .....   | 39 |
| 4.1. Test of Systems of Third Parties (Service Providers, Deliverers and so on) ..... | 39 |
| 4.2. Forensic Analyses (FORENSIC) .....   | 40 |
| 4.3. Check of Organisational Requirements: REVIEW .....                               | 41 |
| 4.4. Individual Issues: INDIVIDUAL .....  | 42 |
| 5. Basics of Security Tests .....   | 42 |
| 5.1. Limitations of Security Tests .....  | 42 |
| 5.2. Comparison between Security Tests and other Examinations .....                   | 43 |
| 5.3. Ten Tips by Sebastian Schreiber: .....   | 43 |
| 6. About the SySS GmbH .....  | 44 |
| 6.1. The Company's History .....  | 44 |
| 6.2. The Special Way to Proceed .....   | 44 |
| 6.3. Tools .....  | 46 |
| 6.4. Fundamental Ethics for Penetration Testers .....                                 | 47 |
| 6.5. Description of Technical Risks during Tests .....                                | 48 |
| 6.6. Publications of the SySS GmbH (Samples) .....                                    | 51 |

## 1. Summary

This guideline relates to approximately ten years of experience of the SySS GmbH when performing security checks both in large multi-national and in traditional mittelstand<sup>1</sup> companies and is based on the wide range of our consultants' experiences and on the intensive communication with our customers.

Security checks and penetration tests are, according to the SySS GmbH, an active quality control of IT security. Within this area our main competence is the check of classic networks, web applications and WLAN.

This paper is aimed for assisting you in selecting the appropriate test items and the respective testing procedure from our offer. We will describe which preconditions are necessary for a positive, efficient and successful performance of a test.

We will also show which decisions and measures are necessary so that the test may also be perceived internally as an outstanding and positive rendition of service.

## 2. Possible Arrangements

Due to the fact that IT systems run in a lot of different ways, security checks cannot be performed by just one standardized procedure. Therefore, they have to be dealt with flexibly and the way to proceed depends on several factors, such as:

- The perspective from which the test is being performed (see *Test Perspective*, p.7)
- The way to deal with *DoS (denial-of-service)* potentials (see *Aggressiveness*, p.8)
- The internal coordination of the project schedule (see *Announced and Unannounced Checks*, p.9)
- The systems and web applications which are to be tested (see *Object to be Tested*, p.4)
- Possible key aspects (see *Test Depth*, p.5)
- Regularity of tests (see *Test Frequency*, p.5)

---

<sup>1</sup> Mittelstand: German for medium-sized enterprise, see: <http://en.wikipedia.org/wiki/Mittelstand>

- Special circumstances during the procedure of the test (see *Hidden or Open Tests*, p.10)
- Selected test modules (see *Project Modules*, p.10)
- Granted budget

## 2.1. Object to be Tested and Test Coverage

Both when performing external (module INTERNET) and internal tests (module LAN/WAN), the objects of the test are systems and their IP addresses. The customer selects a representative sample of the total number of IP addresses. The number of addresses to be tested is called test coverage.

When testing web applications (Module WEBAPP), the object of the test is a web-based application and its functionality.

When checking WLAN, the object of the test, however, is the WLAN of the location of the customer. The coverage of this test describes the size of the campus to be examined and the number of locations and buildings to be checked.

Test object and test width will be taken into account when compiling the offer. We will also calculate our time need. According to the variety of systems and applications, which could be of use in all possible cases, it is very difficult to give you general information. We therefore give you the advice to discuss your object to be tested directly with us beforehand.

In general – especially in big companies – it is not possible to check the entire internal or external network within the test period. Therefore, it is sensible to select some systems.

A special form could be that the SySS GmbH selects samples independently from one or several networks.

If either the customer or the SySS GmbH realize during a test that alterations could be sensible, it is possible to adjust these changes in a non-bureaucratic way given that they do not alter the test duration. These adjustments will take place in direct agreement between the consultant in charge and the contact person of the customer.

## **2.2. Test Depth**

The test depth is the automatic consequence of the chosen test object and the time available. If one of the goals of the test is to gain an overview over a big number of systems in a relatively short time, for instance, the test depth will be rather low and the search for very high risk potential will have priority. If, on the other hand, there is sufficient time for just a few systems available, it is as well possible to also record misconfigurations, which may not be direct security flaws.

The main focus of the test object as defined in the offer will be discussed at the kick-off meeting. The general goal is to state the current security level of the test object within the test time window and to portray which security holes are imminent risks. It is the norm that the consultant in charge will invest more time into detecting security flaws – which enable third parties to intrude – than to deal with errors forming only minimal risks.

The ultimate goal is to get an extensive overall picture of the security level of the test object to clearly name any risks and make suggestions for a remedy. This all happens by way of a report (module DOCU).

If there is the urgent need to change the main focus during the test or to change the test depth, this can be done after a direct conversation between the consultant and the contact person. As a security check is never a linear process, the SySS GmbH offers the necessary flexibility.

## **2.3. Test Frequency**

Security checks will not have an influence on the security process if they only happen once – for the measures which will be executed after a test to remedy any detected security flaws should become part of the members of staff's work routine.

In order to obtain effective results, a security test should be fully integrated into the security process and be performed steadily. Companies attaching great importance to IT security draw up test plans reaching far into the future:

|  | Q2<br>2009 | Q3<br>2009 | Q4<br>2009 | Q1<br>2010 | Q2<br>2010 | Q3<br>2010 | Q4<br>2010 |
|--|------------|------------|------------|------------|------------|------------|------------|
| Security test of systems in the Internet (module INTERNET) |            | X          |            |            | X          |            |            |
| Examination of web applications (module WEBAPP)            |            |            | X          |            |            | X          |            |
| Internal penetration test (module LAN/WAN)                 |            |            |            | X          |            |            | X          |
| WLAN Test (module WLAN)                                    | X          |            |            |            | X          |            |            |

When setting up such a plan it is important to take the permanent change of IT networks and applications into account. The scheduling should be revised and updated approximately every half a year. Furthermore, every test for each respective test object should be chosen in order to have a maximum of benefit and to prevent a negative routine to occur. Vulnerabilities can only be identified by a long-term test plan, thus quality management can be demonstrated.

## 2.4. Expertise of Security Testing

When performing a security test, one both takes up a certain perspective (see *Test Perspective*) and assumes a certain expertise of a potential perpetrator. The SySS GmbH generally orientates itself roughly by the Black-, White- and Greybox Model.

### “Blackbox“ Model:

According to this model, the customer only obtains minimal information about the test object.

A “Blackbox” test should not be misunderstood as a test where there is no information flow between tester and customer and where goals are entirely selected and checked independently.

Before the test, it is vitally important to verify whether a test of the system or of the network is a sensible measure respecting organisational and technical matters.

If a selection turns out to be elaborate, perimeter detection may be executed (module PERIM). Therewith, the SySS GmbH identifies test goals rather independently. Results and the selection of samples will of course be discussed with the customer who determines the release of the test and procures all necessary licences.

**“Whitebox“ Model:**

Within this model, extensive information about the test object is transmitted. Normally, it is not necessary to have this abundance of information within the module INTERNET.

**“Greybox“ Model:**

Security tests of the SySS GmbH generally fall into this category. The customer supplies exactly the amount of necessary information to us so that we are able to perform a security test. If further information is required, we will get back to the contact person of the customer company.

Any kind of information being essential for the test module will be named under “Customer’s Assistance”.

According to many years of experience by the SySS GmbH, this method is considered to be the most efficient one.

## **2.5. Test Perspective**

Different positions, which a potential perpetrator may take up, need to be covered by different procedures.

Thus, one can check which infrastructure is available from the Internet at all. With this information one can estimate the risk of the system being a target for attacks (module PERIM).

In case we should check which risks directly emanate from reachable systems on the Internet by non-privileged users, these systems will be tested externally (module INTERNET).

A web application test is different. Primarily, it is performed from the perspective of regular users (in contrast to unregistered visitors) of web based applications although it is performed

from the Internet (module WEBAPP). This test also deals with the perspective of not registered visitors.

The security test in the internal network (module LAN/WAN) checks the company's network from the perspective of an internal perpetrator. Hence it has to take place at the actual object. When performing internal tests, a lot of systems, which in turn offer an enormous number of services, are reachable. Therefore, the way to proceed will differ from external tests. Among other things we will concentrate on detecting severe security flaws which can easily be exploited.

Security tests of WLAN (module WLAN) are performed from the perspective of a perpetrator in reach of the WLAN aerial. During this test we will examine whether unauthorized use of a network is possible or whether existing connections may be compromised. In the same way as the internal test, a WLAN test has to take place on-site.

## **2.6. Aggressiveness of Tests**

*DoS (denial-of-service)* potentials are very important. On the one hand they can occur by errors in services itself or on the other hand by misconfigurations.

Generally, it is not the aim of security tests to suspend systems or applications but to show such origins of danger (unless the customer explicitly wishes it).

The following procedure to detect *DoS* potentials has proven to be effective: If potentials are being found, we get in touch with the contact person of the customer first. In direct conversation we decide if the SySS GmbH should actually provide evidence (i.e. cause a perturbation) or not. Exploiting *DoS* potentials may be sensible if the customer wishes a proof that it is necessary to alter some constituents of a certain system (maintenance, separation or replacement).

In order to reduce any effects of perturbation which may occur as a result of a *DoS* potential, the following measures may be taken into consideration:

- Tests are best performed at times of lower network load, i.e. in off-peak times,
- evidence of test systems (if available),
- if the potential is being detected in a number of cases, selection of samples.

Additionally to the performance, a person in charge of the system has to be at hand.

Tests opting for a paralysation of networks by using the entire bandwidth are not performed by the SySS GmbH. The risk of such attacks exists at any time and may be determined when considering the given bandwidth.

As a security test is an active control, a perturbation of the systems to be tested can never be entirely ruled out. Detriments can either occur on the functions of singular services, the tested service itself or the entire system being tested.

During the test of web applications, one does not primarily assume *DoS* potentials. But as there may be requests to the data base in the course of the test, which regular users do not generate, these risks also exist here. Therefore, it is difficult to foretell such difficulties. If there are clear indications, we may proceed in the same way as described above.

A security test without potential risks is not possible.

According to the SySS GmbH's empirical value, there are two main reasons for *DoS* during security tests: On the one hand there are often systems and applications not being able to even deal with a moderate load of a test and on the other hand there often are very old and badly maintained services.

If and how to test old and very old services (with a patch level of the year 2000 or older) should therefore be always subject at the kick-off meeting. The same applies to load problems in general. In order to get around the latter problem, it can be agreed on to perform certain tests in off-peak times.

## **2.7. Risks When Performing Security Tests**

Penetration tests always come along with an unavoidable risk which only differs in certain aspects from function, load or connection tests. In the same way like with those tests, a security check has to face a certain data volume which the involved systems have to deal with in their normal work process.

The main difference to other test procedures is that during a security test, certain services are confronted with enquiries not occurring on a daily basis.

This is exactly the basic procedure when detecting all kinds of security deficiencies. There is no alternative to this proceeding unless one would like to do without any technical measures at all.

In order to avoid as many risk potentials as possible, the SySS GmbH proceeds in the following way:

- Test performance by examined and experienced specialists
- Performance of penetration tests only after a written commission
- Check of data delivered by the customer for correctness (e.g. IP-Ranges). In case of a lack of clarity, the customer will be consulted
- Kick-off workshop according to a proven check list including minutes taken
- The SySS GmbH's customers are always correctly informed about any possible risks before placing their order; during the on-going project they will be looked after to the best of abilities.
- Risk minimization by carefully designing the test project: Slow scans (reduction of bandwidth), however, increase the test duration.
- Tests can also be performed besides office hours (e.g. at night time/weekend). If the customer explicitly wishes such a proceeding, a contact person of the customer's company must be at hand during the entire test time.
- Analysis of test systems; if the test system does only correlate with the productive system in a few points, the SySS GmbH will clearly indicate to this fact in the report so that its informative value will not be falsified.
- When difficulties occur, the test will immediately be broken off. Problems which are created indirectly are often not recognized by externals. Therefore, the contact person of the customer company should be able to clearly relate problems to the test and above all inform the SySS GmbH.
- The chosen test methods are non-invasive. The result is that there will be a certain reduction of the gain of knowledge which has to be taken into account. Speculations of any kind will always be marked as such in the final report by the SySS GmbH.

The SySS GmbH would like to emphasize once more that it is essential that a contact person is always available during the test, for without him/her a number of the points stated above cannot be fulfilled.

Above all, the contact person should have the competence to plan an alternative test course or change the focus of the test if need be. If organisational proceedings do not take such changes into account, they should be altered. In case the usual contact persons are not available at some stage during the test they have to appoint delegates and grant them full authorization.

Due to the experiences of the SySS GmbH, there are four technical causes on which all the risks are based. These causes will separately be dealt with in chapter 6.5.

## **2.8. Announced and Unannounced Checks**

The approach of penetration tests are targeted on technical but by no means on human deficiencies. Unannounced tests, however, are often perceived as such by those involved. Therefore, such tests have the disadvantage of often being questioned and doubted and the motivation of members of staff is getting very low to put urgent security measures into practise. The goal of a security test is often not reached by performing tests without announcing them beforehand.

The lasting success of the SySS GmbH is to build up confidence with contact persons, engineers in charge of the system and administrators instead of distrust. One main issue is to offer to everyone involved to personally attend the test.

### **Tip by Sebastian Schreiber:**

Communicate with all your members of staff involved about the planned tests. Therewith, security tests will be understood as a useful rendition of service and the results will efficiently be put into practice.

## 2.9. Social Engineering

Besides all technical possibilities and options, *social engineering*<sup>2</sup> is one of the most effective means to obtain sensitive data. *Social engineering* originally means “Applied Social Studies” but the term is applied when referring to “social manipulation” and comprises professional defraud. The impostors often masquerade as entitled technicians or external service providers and thus manage to request the wanted information successfully. Normally they have a good knowledge about the business culture in order to be able to exploit bustling situations brazenly (e.g. major IT changeovers, moves, etc.).

Although *social engineering* is one of the biggest dangers for companies and the discussion about measures for narrowing down this risk potential is certainly legitimate, there is a crucial difference to all other test methods: Test object in this context is man and not a technical component. But as man is not to be equated with a technical device working impeccably, members of staff do often react very sensitively to this topic and therefore often have a very critical attitude towards tests of this kind. For the most part they see such tests as ethically questionable and solely perceive them as inhumane control measures often doing more harm to the company than strengthening its internal security.

Furthermore, a tester has to take on a false identity and thus lie to members of staff on purpose or knowingly lead them astray. From a legal point of view such tests are critical if they do not apply to strongly controlled conditions. Besides a legal protection of the tester, it has to be granted that the works council, too, agrees to such tests of behaviour.

Due to the reasons given above, the SySS GmbH recommends only to take *Social Engineering* tests into consideration in exceptional cases.

## 2.10. Hidden or Open Tests

The performance of security tests is – as already mentioned – not hidden. The leading consultant will not implement any measures to hide the test activities. Our experience is that measures being apt for hiding the test from automated intrusion detection and response systems severely increase the test time, much more than is tolerable for a normal procedure of the project.

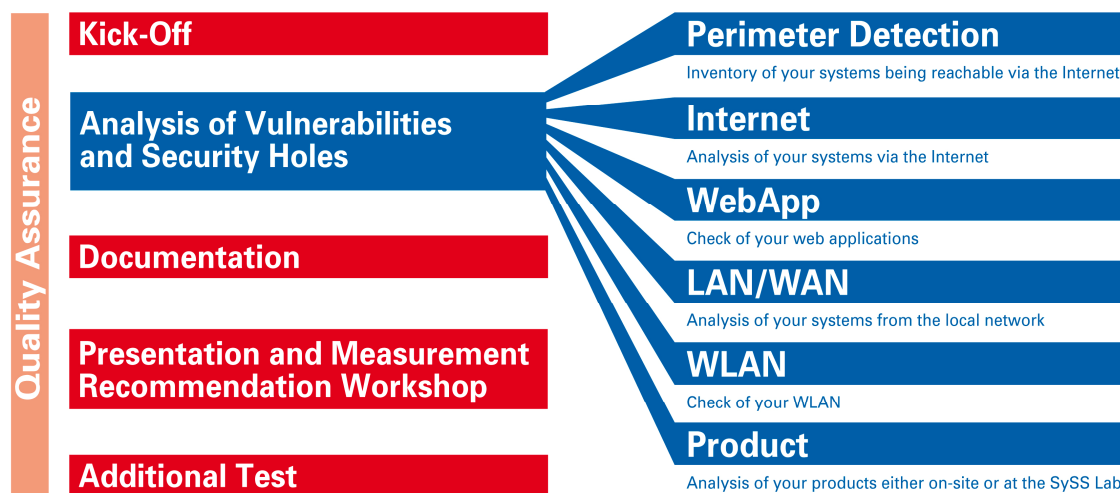
---

<sup>2</sup> See also: [http://en.wikipedia.org/wiki/Social\\_engineering\\_\(security\)](http://en.wikipedia.org/wiki/Social_engineering_(security))

The reports, which will be issued within the documentation frame (module DOCU), will additionally give intelligence about the fact whether automated systems will have recognized the tests having proven security holes with a high risk potential.

### 3. Project Modules

The security test consists of a frame project and singular test modules:



The respective test modules will be described in the following chapters. If your requests are not fulfilled in a satisfactory way, please do not hesitate to get in contact with us. In such cases we are very happy to provide you with your own individual project plan.

#### 3.1. Kick-Off: KICKOFF

In a preliminary discussion (e.g. on the phone) we will talk about the project schedule. The responsible consultant leading the test will discuss the following issues with the customer:

- Time frame of the test
- Contact persons and their availability
- Review of the object to be tested
- Fulfilment of preconditions
- The way to treat the detection of *DoS* potentials

- General information about the procedure
- Defining the language in which the report is to be written (English or German)
- Number of required copies of the report
- Enquiries and requests of the customer concerning the test schedule

According to special objects and to the selected modules, there may be individual changes. Should any changes be necessary when performing the test as being described in the respective sections of the modules, they will be discussed in due time.

Minutes will be taken from the results of the kick-off and soon be made available to the customer.

**Tip by Sebastian Schreiber:**

Before the kick-off, it is important that you check the points and advice listed under “Customer’s Assistance”! The more time you invest into preparing and performing the kick-off, the more efficient the test will be and the more will it be useful for your company!

### **3.2. Perimeter Detection: PERIM**

**Summary:**

The SySS GmbH identifies networks and systems of the customer on the basis of publicly available information. The customer will receive an overview of systems being active on the Internet and belonging to him. He can release those for further tests. Perimeter detection supports internal inventory measures and the selection of systems to be tested for further modules.

**Starting Position:**

The total of all systems of a company being reachable via the Internet is called perimeter. Normally, security tests are only performed on IP addresses which have been selected beforehand by the customer (and sometimes with the help of the SySS GmbH).

If it is not possible to have such a selection, especially when the networks of customers are big and divided up internationally, perimeter detection may be executed.

It is the goal to compile a list of networks, which may easily be attributed to the customer, to discover possible additional errors during the attribution and if appropriate to choose suitable candidates for a test. The latter takes place by the customer's verification itself. The customer also has the opportunity to correct errors in his own documentation or ask a service provider (ISPs) for it. Due to the legal framework, the SySS GmbH cannot act independently, but in any case it must be prevented that third parties are affected.

Reasons for this could be:

- Undocumented outsourcing of IP addresses to third parties
- Old or erroneous WHOIS entries
- Common use of systems with third parties (e.g. web hosting)

Therefore, the customer has to release all networks and systems to be tested.

Other sources for perimeter detection are – besides the freely accessible data bases (WHOIS, DNS) – the customer's mail routing and contents of websites which could to some degree shed light on any corporate links.

#### **Precondition:**

In order to distinguish the customer's systems from those of third parties and to be able to synchronize any results with the existing documentation, a contact person should be available during perimeter detection.

### **3.3. Analysis from the Internet: INTERNET**

#### **Summary:**

Systems of the Internet are examined for definite security flaws and risks thereof are evaluated. Within the documentation frame, a catalogue of measures will be suggested for remedying any recognized vulnerabilities.

### **Starting Position:**

There are two kinds of risks when using systems on the Internet. On the one hand security flaws may exist in some of the systems enabling third parties to

- obtain detailed information about systems, which may be of use for further attacks,
- enter into the system and use it for their own purposes or for further attacks or
- the possibility to manipulate data, which should not be allowed to be altered by third parties.

On the other hand there is the danger that data from the Internet may be of use for attacks without being intended so. This danger can emanate from:

- Acquisition of information about systems and the software being used, which may be critical information for other attacks (*information leaks*),
- indication of the names of user accounts,
- confidential data and information not relating to the system and the software in use.

The opportunity to obtain information should not be underrated as security holes may be exploited in combination with just these hints.

### **Goal of the Test:**

The goal of a security test within the frame of the module INTERNET is to check the respected systems for any risks mentioned above depending on the test depth. The aim is to specifically detect any security holes and to find data which can be exploited and monitored by an unrestricted circle of users (Internet public). As described under section “Aggressiveness”, it is not the aim to paralyse systems or services but just to detect such potentials.

Web applications are not checked within the frame of the module INTERNET, if you request such a check, see module WEBAPP.

Furthermore, we will try to get a general overview about the present security level in a simple comparison with other examined networks. An analysis of value of any kind of data found will not be executed as our experience has shown that customers can do such analyses very well themselves.

### **Performance:**

The way of performance will be determined by the leading consultant but generally the following scheme is observed:

- Check whether data being made available by the customer are correct
- Identification of operating systems and available services
- Test of detected services with vulnerability scanners
- Check of results, verification of detected security gaps
- Use of tools, which cover areas not being able to be taken into account by vulnerability scanners
- Manual examinations
- Proof of *DoS* potentials by arrangement with the customer

According to the existing information, the testing consultant chooses the appropriate tools supporting his work best. Some examples may be found under the section “**Tools**”.

### **Customer’s Assistance:**

In order to perform a security test efficiently and beneficially for the customer, some parameters have to be fulfilled. Otherwise, the test may become difficult or be delayed.

- Systems must actually be reachable via the Internet.
- The addresses of the systems to be tested must be available when starting the test.
- When choosing the test time (within the kick-off), maintenance windows, dependence on time zones (when testing systems abroad) and bank holidays have to be taken into account.
- Contact persons should be available during the entire test time.
- The contact persons should have a general overview over internal responsibilities of the systems to be tested; this reduces the amount of communication during the test.
- IDS/IPS systems should not block the systems to be tested.
- Responsibilities should be clear.
- For testing systems of third parties, a written consent must be on hand.

**Tips by Sebastian Schreiber:**

Make sure that members of staff and those in charge of the systems are informed beforehand that the test may be received in a positive way.

You can increase the quality of the test when you have your own documentation about the addresses to be tested checked before the start of the test.

### 3.4. Check of Web Applications: WEBAPP

**Summary:**

Selected web applications are tested from the user's perspective for their security. Security holes will be looked for depending on the used software, its configuration and application logic.

**Starting Position:**

With web applications there is a high risk of losing confidentiality when unauthorized persons access data. Additionally, the communication with the user is relevant, especially as both external and internal users may be threatened by *Cross-Site Scripting* vulnerabilities.

There could also be security flaws which may cause malicious alterations at web applications or its elements.

Similarly to the module INTERNET, risks consist of the intrusion of third parties and the possibility of (unsolicited) information transfer.

A speciality of web applications is the generally complex dependences on other systems, e.g. e-mail and data bases – these may also get infected by vulnerabilities in an application. Information can be gained from the data bases as well.

These dependences can rely on used middleware, too, and in an organisational way on deliverers.

Furthermore, the security of a web application is not only determined by the application itself but also by the CMS in use.

Another special feature of web applications is that amateurs may track vulnerabilities once they are made known; therefore there is the danger of damaging one's reputation and the loss of confidence.

### **Goal of the Test:**

The goal is to check whether any of the risks mentioned above are existent. The evaluation of the risk of individual vulnerabilities is more significant in this test as the existence of a general problem does not necessarily indicate to a special risk.

Moreover, the main focus of the test is to see whether the exploitation of typical security flaws of web applications enables the inspection of other users' data.

Finally, the security level will be estimated and measures for remedying actual vulnerabilities suggested.

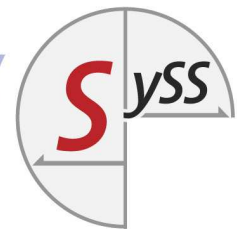
### **Performance:**

The test performance depends very much on the function and structure of the respective web applications. Therefore, it is not possible to lay down a fix scheme for the test procedure. Nevertheless, it roughly follows the following pattern:

- Getting a general idea of the divers functions of the applications
- Detection of possible risks and starting points for attacks, e.g.
  - Takeover of different/inaccessible functions
  - Inspection of different identities
- Access to closed data
- Manual review of such risks/starting points
- Search for more starting points

In addition, the following examinations may take place if requested:

- Analysis of the session concept
- Search for unsolicited released information
- Security check of the CMS if at hand



Vulnerability scanners and those which have been provided for the test of web applications are rather of a supporting nature as they are not capable to use and evaluate information alluding to the context.

### **Customer's Assistance:**

For the test, it is inevitable that the customer passes on the URL of the web application (regarding access data, see below). It should be taken into account that the CMS in use will be tested as well.

### **Contact Persons:**

The analysis of web applications does not only differ from other test modules regarding its procedure. As already described, security problems in web applications can also affect other services.

Besides, web applications and their functionality generally do not stem from one source: The design may come from an external agency while the programme of the web application is generally written by either internal or external software engineers.

In order to remedy detected security flaws it is vital that the customer gets in touch with all those who are in charge of the affected elements. Therefore it is of great importance to know the contact information of all involved parties to be able to get in touch with them if necessary.

If there are no direct contact persons, two problems may arise:

- Enquiries during the test – which may be useful for the verification of vulnerabilities – may result in delays as there is nobody there to deal with them.
- If the persons responsible for a project, which is affected by security flaws, are not known, a possible remedy may be delayed strongly.

This is the reason why it is important that responsibilities are clarified well on time before the test, even if this step seems laborious at first.

After that, everyone concerned should be informed about the date and the objective of the test. They are also very welcome to attend the test if they wish. If third parties are concerned, they have to agree to the test (by a letter of agreement).

Additionally, one contact person, who is well acquainted with the web application from a user's perspective, should be available for any further queries.

### **Dependences:**

Any detected organisational and technical dependences should be communicated to the SySS GmbH. This can take place during the kick-off.

### **Status of Web Applications:**

The functions to be tested should possibly be available at any time. In an early or medium early stage of implementing a new web application, a test may not yield effective results. Nevertheless, it can be sensible in order to get decision-relevant results.

### **Access Information:**

The SySS GmbH requires two user accounts at least per authorization level out of which the test shall be performed. If such accounts are not available, a test may only be performed from the perspective of a visitor. This does not often give any intelligence about the security level of a web application. In order to obtain useful results, the rights of those user accounts must not be restricted compared to the ones of regular users. The way how to generate these accounts will be discussed during the kick-off.

### **Test Data/Test System:**

If the test should not be performed on productive data or systems, we can also work with a productive system with test data or just with one test system. In this case test data files, which could be accessed by the user accounts needed for the test, should already be provided before the test start.

When working with pure test systems, the result of a security test is only significant if its functionality corresponds in vast parts with that of the productive system.

### **Tips by Sebastian Schreiber:**

In order to remove any detected vulnerabilities during a web application test, you need the cooperation of the person who is responsible for the affected element. Therefore, try to ascertain everyone in charge as early as possible and inform them about the test – this is the only way to guarantee a quick reaction.

We also consider it as vital that you inform everyone being involved, also those who do not play an active part during the test. By doing this you increase your members of staff's confidence in the rendition of service of the security test and you strengthen the position of your IT security within your company.

If there is no access information available for us, a test then is only of little significance.

### **Test Tools and Exemplary Vulnerabilities:**

The analysis of web applications can be supported by the use of vulnerability scanners. We use, among others, NESSUS, CORE IMPACT, MAXPATROL, SAINT, BURP SUITE PROFESSIONAL and – if the customer bears the license fees – APPSCAN (WATCHFIRE/IBM). The use of APPSCAN is a sensible measure, especially when testing complex applications or when a high number of applications are being tested during a project.

The effectiveness of security scanners is limited at this particular point. This is the reason why the main tool for checking web applications is always an Internet browser, with which it is possible to perform manual examinations. There is a number of plug-ins available for FIREFOX (MOZILLA), therefore it is preferentially used.

Additionally, we also make custom-made tools (e.g. scripts) in order to verify actual security flaws.

### **URL Manipulations:**

When parameters are transmitted to scripts, etc. via the URL within a web application, there is a risk that they are manipulated. In such cases it may be possible to make unwanted requests (e.g. manipulation of prices) or to construct links for *phishing*.

## Examples:

If a web application uses the following URL:

```
http://www.shop.com/shoppingcart.asp?Action=Buy&type=special&price=200
```

The price can be modified by way of URL manipulation. If other parts of the website are communicated via URL parameters, as, for instance:

```
http://www.shop.com/index.php?session=xd67u9n&url=/specials.html
```

other sites may be loaded by possible alterations.

```
http://www.shop.com/index.php?session=xd67u9n&url=www.preparedsite.com
```

If it is possible to get an insight into the files of the web server via the information of the tracks shown in the URL, there is a *path* or a *directory traversal* vulnerability:

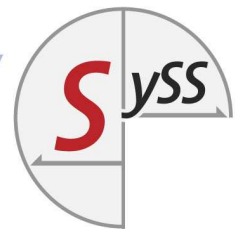
```
http://www.shop.com/default.pl?..\..\boot.ini
```

If it is possible to execute operating system commands via the URL, there is *command injection*.

```
http://www.shop.com/default.pl?angebot;uptime
```

At this point it may also be necessary to code any kind of entries that they can be executed.

The consequences of URL manipulations depend on the respective application. Therefore, the risk will be evaluated individually by the SySS GmbH. URL manipulations only require a browser as a tool and no special knowledge. This is the reason why they are considered to be a high risk for exploitation.



### **XSS Vulnerability:**

If entries in form fields or other changeable parameters are not validated server-side, they can be used to insert code being executed in the context of other visitors. This way of attacking is called *Cross-Site Scripting* – abbreviated as *XSS* – as further code fragments can be loaded from a foreign server by the injected code. Normally, two different forms of XSS are being distinguished: *Reflected* and *persistent XSS*.

When executing *reflected XSS*, the attack vector containing the code to be executed is normally stored in an URL parameter. This parameter is integrated server-side in generating a dynamic website and the inserted code is being executed when a visitor accesses the URL in his web browser.

### **Example for *Reflected XSS*:**

If the URL of a website is accessed containing a vulnerable parameter (in this case: “user“) which is not sufficiently validated server-side but implemented in the dynamically generated website, the code given to this parameter is executed. In this example a JAVASCRIPT popup window springs open containing the text “XSS“:

```
http://www.seite.de/login.php?user="><script>alert('XSS')</script>
```

Thus manipulated URLs are often spread by way of fraudulent e-mails or in freely accessible web forums or blogs.

This is not necessarily the case with persistent XSS vulnerabilities as the code is stored permanently server-side and executed each time the concerned website is accessed. The basic problem however remains just one: parameters which can be altered by users are not filtered sufficiently.

Persistent XSS vulnerabilities are often found in user profiles or communicative functions like forums or blog entries.

### **Example for *persistent XSS*:**

A web application allows users to administrate customer data. The entry of comments like “do not call before 10 am”, for instance, regarding a single customer, is normally not validated. Therefore, the following entry is possible:

```
<script>alert('XSS')</script>
```

Whenever XSS vulnerabilities occur, they can be analyzed to what extent more complex entries are possible enabling *Session Hijacking* (see below), for instance, depending on the available test time. This is not always possible, therefore the SySS GmbH evaluates the risks emanating from XSS vulnerabilities on an individual basis.

Under certain circumstances, XSS vulnerabilities can be detected by security scanners making pre-defined entries. In a lot of cases this is only possible by adjustments to the entries, which security scanners cannot perform – therefore, manual work is necessary.

### **SQL Injection:**

*Structured Query Language* (SQL) is a query language for relational data bases. These data bases carry out the task of saving information in a lot of web applications. User call up data according to the respective input fields and the results are processed by the application. If entries are not checked sufficiently, queries can directly be posed to the data base in SQL; this is called *SQL Injection*.

Within this context one has to analyze whether a respective user can monitor contents which he should not be authorized to read or whether the data base is prone to manipulations.

### **Example:**

The application offers a search mask via which it is possible to search for users respecting their location when internally using the following command dealing with the query for the location “London”:

```
SELECT * FROM user WHERE location='London'
```

As entries are not checked, the following query is transmitted:

```
London' ;DROP TABLE User --
```

Leading to the following SQL command:

```
SELECT * FROM user WHERE location='London' ;DROPTABLE User --'
```

The command “DROP TABLE” extinguishes the table “User” from the data base. The comment character string “--” is used to suppress any further commands. Such destructive tests are not performed during a security test but they illustrate the enormous risk emanating from *SQL Injection* security flaws.

SQL data bases are also used for the authentication of users on the application itself. If entries are not sufficiently checked at that point and SQL commands be directly inserted, there may be the possibility to fully avoid the authentication mechanism.

### **Example:**

The following command is used internally for authentication:

```
SELECT permission FROM users WHERE user= '$user' AND  
pass= '$pass'
```

The following user name is accepted by the application (and not rejected):

```
meier' OR '1'=1
```

This complete query to the data base now has the following form:

```
SELECT permission FROM users WHERE user='meier' OR '1'='1' AND  
pass= '$pass'
```

The original query requires that both user name and password are being given. The logical “OR” having been inserted by manipulation makes this condition optional. If the user name exists in the data base, a successful authentication follows instantly.

Such *SQL Injection* flaws, which allow a complete avoidance of the user authentication, are considered as a high risk by the SySS GmbH. They fully compromise the security of an application.

### **Session Hijacking:**

Another thing which will also be checked is whether it is possible to get access to an authenticated session of a third user and to take over his identity within the application. Such an intrusion to an application is generally manoeuvred by the usage of a session ID. This can be saved locally on the hard disk of the user in form of a cookie, put into the URL or being contained in HTML code as a hidden field.

### **Example:**

```
http://www.example.net/view/7AD30725122120803
```

The best way to steal the session ID of a user is by XSS attacks. Via a *Cross-Site Scripting* (XSS) vulnerability, especially provided commands (e.g. JAVASCRIPT code) can be uploaded by a third system and executed in the browser of the respective user. These commands readout the user's session ID and transmit the information. The user concerned only has to read a modified entry in a forum or look at a description in a product data base on the browser. Normally, the user is not aware that he thus becomes a victim of *cross-site scripting*.

The result of successful *session hijacking* is therefore the takeover of the identity of an affected user within an application. The SySS GmbH always evaluates the possibility of a possible session theft as a high risk.

## **3.5. Security Test in the Internal Network: LAN/WAN**

### **Summary:**

We test systems in local networks for concrete security flaws and evaluate risks going forth from them. Within the frame of the documentation, a catalogue of measures for removing any acknowledged security holes will be set up. The main focus lies on the detection of security holes, which have a high potential for inside perpetrators.

### **On-Site Perspective:**

Two perspectives may be taken up during the test:

On the one hand one can take up the position of a user with access to the internal network. Systems are then examined similarly for security gaps as in an external test.

On the other hand one can take up the position of the user of a definite system (“intern”/“temporary worker”). In this case we will check how well the system (e.g. the standard desktop for the respective user group) is protected against manipulation and if it could be used for attacks.

As there normally are an enormous number of services which could be tested, it is very important to have a choice of expedient samples. This should be discussed during the kick-off meeting.

### **Particularities:**

In internal networks a vast number of services and protocols may be used. The SySS GmbH is therefore competent to test IP-based systems in Ethernet networks.

In case of very big and complex networks, the SySS GmbH are very happy to assist their customers when choosing expedient samples and if need be to do an inventory roughly corresponding to the perimeter detection.

### **Starting Position:**

In contrast to systems of the Internet, whose risks threaten an unlimited circle of users, the Corporate Network assumes risks emanating from inside threat. To be more specific, we think about users with access to the Corporate Network. Such users automatically have a greater knowledge about the network surrounding them due to their position.

Furthermore, there may be the risk of involuntarily dragged-in malicious code. Malicious code can exploit security holes automatically.

Additionally, the risk is much higher when the PC of a user can be utilised.

### **Goal of the Test:**

The goal of the test is to detect and to evaluate any kind of risks depending on the perspective having been taken up and to make suggestions for their removal. When detecting security flaws the potential of inside threat must be taken into consideration. But not only security flaws as such are being analysed but also configurations and the availability of certain software, which may give valuable hints to an inside perpetrator and could grant him a successful attack.

In order to detect *Man-in-the-Middle* potentials, we do not only evaluate the vulnerability of singular systems but also the communication of services among each other.

We suggest that systems may be partitioned off internally if other security measures (update, replacement) are not possible.

The SySS GmbH does not perform an organised check of data access authorization. Such controls cannot be exercised by externals.

### **Performance:**

In principle, the performance of this module is similar to the module INTERNET:

- System check for available services
- Test of services with automatic vulnerability scanners
- Verification of results
- Supportive and manual examinations
- If need be, check of the used protocol for *Man-in-the-Middle* potentials

A speciality is the examination of a workplace. Herewith we test whether direct manipulations of hardware are possible (booting of external media) and then which possibilities the operating system offers itself.

Systems are often used in internal networks which have never been designed for the Internet or which have been used for a very long time, sometimes even beyond their lifecycle. The risk of crashes when testing such systems is very high. Therefore, it is inevitable to cooperate closely with a contact person.

The SySS GmbH generally recommends to test systems, which have reached the end of their lifecycles or which have not been maintained since the year 2000, only if the direct confirmation is needed to partition off such systems or to replace them and if the consequences of any kind of occurring damage is hazarded. If possible, systems should be chosen for these tests, which do not fulfil a critical function. We abstain from any liability claims by our general terms and conditions for all potential crashes or other interferences if damages are caused.

### **Customer's Assistance:**

Certain logistical preconditions must be fulfilled for an internal test as the test is not a self-sufficient rendition of service.

### **Contact Persons:**

A contact person should be available during the entire span of the test time. He may also attend the test. As the test takes place on-site, all organisational framework requirements must be met before the start of the test.

### **Information for Everyone Concerned:**

Everyone being responsible for the system, all administrators and all other members of staff concerned should be informed about the test and its purpose before the start of the project. Their cooperation may be valuable during the test and is of crucial importance for remedying possible vulnerabilities.

### **Workplace:**

The consultant should have his own workplace at the company. The following items are necessary when a network is being tested:

- Two network access ports (Ethernet) to the network to be tested
- Electricity supply for two notebooks and a switch (6x multiple socket)
- Enough space for two notebooks, switch and documents

For the test of a workplace, it is essential to have space and electricity for a notebook and Internet access (documentation and research).

If any permission is necessary to run one's own hardware at the workplace, it should be at hand well on time before the start of the test.

### **Access to Buildings:**

The consultant should be able to enter the respective building on the day of testing with all his equipment and be able to reach and to set up his workplace as described above. All permissions which may be necessary should therefore be asked for in due time.

### **Tips by Sebastian Schreiber:**

You can enhance the result of an internal test on a qualitative level by taking your time and a lot of care when selecting the systems to be tested.

On a lot of identical systems a profound test of two samples is in most cases wiser than just a rough test of all.

The goal of a security test is to detect technical deficiencies. Therefore it is important that you inform everyone concerned before the test so that members of staff perceive the test as a positive activity sustaining the security of your company.

## **3.6. WLAN Test: WLAN**

### **Summary:**

The customer's WLAN will be analysed for security flaws on-site. Additionally, the client security will be checked. Within the frame of the documentation, the security level of WLANs will be described and suggestions be made for remedying security flaws.

The SySS GmbH views WLANs as radio networks according to the IEEE standards 802.11a/b/g. Other radio networks (based on OWL, OPENAIR, UHF, S-UHF, etc.) are not part of a WLAN test.

### **Starting Position:**

WLAN can be reached and received by third parties at any time in contrast to wired networks. Therefore, the WLAN infrastructure is prone for abuse. On the one hand the threat consists in unauthorized use of WLAN and on the other in the danger of unauthorized persons being able to spy out transmitted data. The part of the company network being reachable via WLAN is thus affected.

### **Goal of the Test:**

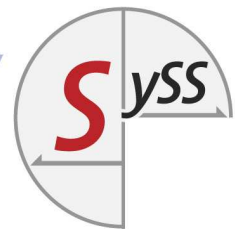
In order to exclude the risks mentioned above, both access points and WLAN clients (notebooks, for instance) will be analysed. The main focus of the analysis will be the encrypting and authentication method in use as well as the client configuration. When doing such an analysis we put our main emphasis on the resistance against *Man-in-the-Middle* attacks.

Additionally, an inventory of the WLAN may follow, in which we check its configuration.

### **Performance:**

The WLAN test necessarily has to take place on-site. The exact procedure depends on the location(s) to be tested and the WLAN infrastructure in use. The proceedings are roughly as follows:

- Verification: Do the issues found conform to expectations/information?
- Detection of access points
- Analysis of networks concerning authentication and encryption
- Attack against the detected authentication and encryption
- Analysis of WLAN clients



When analysing WLAN clients, a DoS is an essential part. But this, however, may be restricted to selected systems (e.g. reference client).

A selection of possible test tools will be presented under “**Tools**”.

### **Customer’s Assistance:**

As WLAN tests always have to take place on-site, it is inevitable to have a permanent contact person at hand.

### **Information:**

Before starting the test, any information about the WLAN infrastructure, especially the type of access point in use and the way of authentication, should be made available. This is best to be done within the kick-off meeting.

Furthermore, everyone concerned, as well as those being responsible for the WLAN system, should be informed about the test and its intention and be available during the test for any questions.

### **Contact Person:**

The Contact Person should be easily approachable and be able to grant the consultant access to the buildings to be tested. Our experience shows that it is most efficient if the contact person himself has all access authorizations and is able to issue them himself.

If the consultant was to test locations without being attended to, there should be one person per location available granting him access to buildings and sites and providing all necessary documents for the consultant.

### **Access to Buildings and Sites**

All necessary permissions must have been obtained on time and be present when starting the test. This applies for the access of the consultant himself as well as his equipment.

When choosing the time frame, opening hours and general working times should be considered especially.

If WLAN clients are to be tested, reference clients must be available or samples selected.

In case there are several locations, which should be tested in one day, it is important to also consider external criteria when choosing the time frame and the duration of the test.

**Tips by Sebastian Schreiber:**

Get hold of all necessary permissions for the access to buildings in due time and inform everyone concerned. By doing this you can avoid unproductive delays.

It is important to inform everybody concerned as only then the test may be perceived as a positive activity and not as an irritating control mechanism. Invite especially those of your colleagues, who seem to have the highest concerns, to attend the test.

### **3.7. Product/Laboratory Tests: PRODUCT**

This test serves examination purposes whose depth goes beyond the check for manipulation or a reference workplace within the borders of the module LAN/WAN. Test object are both multifunctional client and server systems and also systems for special tasks (ATMs, control systems, Internet kiosks, etc.). The test perspective taken is the one of a person having physical access to the system. The test coverage has to be defined beforehand. A typical scenario is the evaluation of a risk emanating from theft of the system or an intrusion at the system's depository. Another one, however, is the review of the risk by way of misuse by a regular (malicious) user of the system.

**Performance:**

The performance is completely dependent on the product to be tested and will be discussed during the kick-off. According to complexity and kind of the product, it is difficult to estimate

the expenditure of time; generally, the main focus of the test is the identification of high risk potentials.

Active tests are only performed during a product test and on the test version itself. The test will not be extended to other systems of the customer without consulting him and without a direct order. If dependent systems are to be tested, this can be done within the frame of the suitable module (INTERNET, LAN/WAN, WLAN, WEBAPP).

Main target is to look for security problems, which are exploitable without causing severe and lasting damage and thus remaining undiscovered. Similarly to the search for *DoS* potentials, the leading consultant will confer with the customer before performing tests which could cause damages to the object.

#### **Customer's Assistance:**

In order to perform such a test, logistical preconditions must be fulfilled. Either transport or access to the test version has to be organised and as at other tests, contact persons have to be available for enquiries (a contact person should also be acquainted with the handling of the test version itself).

If the test version is not a completely autonomous system, which can be tested separately from other systems, it has to be determined during the kick-off, which tests should be performed on dependent systems and which contact persons are available.

During the kick-off the customer should inform the SySS GmbH about the operating system in use on the systems to be tested.

Additionally, it should be defined whether the main focus should be on the communication of the system or whether software and hardware can be manipulated.

#### **Tips by Sebastian Schreiber:**

Estimate the expenditure of time for a product test very generously!

Check with which systems your product communicates – normally a complete test of these systems is sensible if it is an organisational and technical unit. Afterwards choose the suitable module for the test.

### **3.8. Documentation: DOCU**

The results of the performed tests of the previously described modules will be documented in a report. The report contains the following points:

- Summary of all results and evaluation of the general security level (“Executive Summary”)
- A list of all detected vulnerabilities together with an approximate estimation of the risks thereof and measures for their remedy
- Comprehensible portrayal of every proof of a detected security flaw
- Extracts from the issues of the working tools where this information makes sense
- Anomalies during the course of the test
- Evidence of the communication with the customer if necessary

The customer tells the SySS GmbH how many copies of the report are wanted.

The report will be printed and bound by the SySS GmbH in-house. It will be sent to the customer as registered mail with a return receipt (also when sending reports abroad). Additionally, the customer will get the report as a PDF-file.

If the customer wishes, he may get all revealed raw data (issues of test tools) having emerged during the test on CD/DVD. But this data will only be made available unprocessed; thus false-positives, for instance, may not be removed from the results of a vulnerability scanner.

If not agreed otherwise, raw data are always deleted three months after the end of a test or three months after a possible additional test.

When performing internal tests (LAN/WAN), more documentation is required as the progression of such tests has to be described in more detail. Any measures for removing security flaws are generally discussed with the contact person during the documentation process.

This is an example of a list of vulnerabilities and recommended measures:

### 1.3 Found weaknesses

| # | Topic  | Recommended measure  | Risk   | Reference          |
|---|--|--|--------|--------------------|
| 1 | webapp.company.de:<br>Method PasswordChange: Session Hijacking possible via XSS.                               | Validate parameter "orig" and deal with special characters respectively. | high   | 3.2.4.2<br>page 22 |
| 2 | IP 127.0.0.7:<br>Apache Version is vulnerable for diverse security holes .                                     | Check the version in use, execute an update, if possible.                | medium | 2.2.5<br>page 12   |
| 3 | IP 127.0.0.7:<br>OWA vulnerable for URL Injection.   | Check issue and update version.  | medium | 2.2.5<br>page 12   |
| 4 | webapp.company.de:<br>DoS attacks possible with smaller loads.   | Stabilize the application, verify the backend capacities.                | medium | 3.2<br>page 17     |
| 5 | webapp.company.de:<br>Method PasswordChange: Phishing Attacks possible by URL Injection.                       | Only allow relative links for parameter "orig".                          | medium | 3.2.4.1<br>page 20 |
| 6 | IPs 127.0.0.{3,4,5}:<br>Loadbalancer can easily be bypassed, therefore direct unencrypted access on webserver. | Block direct access to server!   | low    | 2.2.3<br>page 11   |

### 3.9. Presentation Workshop: PRES

The results of the entire test can be shown to the customer on-site by way of a presentation with the character of a workshop. The following bipartite procedure has proven to work very well:

The presentation begins with a briefing for the decision-makers ("Management Summary") of 30 minutes maximum. Fundamental results of the test will be talked about on a strategic and organisational level.

If you wish, the Managing Director of the SySS GmbH himself, Mr. Sebastian Schreiber, will be available for this part of the presentation.

The second part will be a technical workshop for those being responsible for the system and administrators. In this part all participants have the opportunity to raise more profound questions and discuss possible solutions. This part will be conducted by the consultant in charge of the test.

### 3.10. Additional Test: RETEST

#### **Summary:**

The additional test carries out the task to estimate the effectiveness of remedial measures for vulnerabilities, which have been detected in preceding tests.

#### **Starting Position:**

After identifying security holes by a test, a remedy must follow. In order to do that, the SySS GmbH does not normally have to give special advice – the results of these remedial measures, however, should be verified.

Therefore, an additional test should be performed 2-4 weeks, but half a year at maximum, after the main test.

Such a test does not look for new vulnerabilities but checks the status of the already known flaws and documents everything.

The procedure will be discussed shortly beforehand.

The documentation will be an adjusted version of the report of the test already known.

#### **Customer's Assistance:**

#### **Contact Person:**

If possible, the same contact persons should be available during the additional test as during the first.

#### **Tips by Sebastian Schreiber:**

Schedule the additional test on time and add it to the test plan as a fix appointment!

If the additional test is conducted shortly afterwards, it serves the security level best by positive results, for the remedial measures will thus be confirmed.

## 4. Special Examinations

### 4.1. Test of Systems of Third Parties (Service Providers, Deliverers and so on)

Systems and networks forming a unit can both from organisational and law's perspective be serviced and cared for by several companies and therefore they are also owned by them.

Complete systems can be rented from web hosting systems, for instance, or the used spam filter system may be a service offered by third parties. Furthermore, systems and also whole networks can be used by several companies at once. The special interrelations at web applications are described in the module WEBAPP.

On the one hand it is sensible to consciously check the whole system and thus to include systems of third parties, on the other hand such interrelations are often not obvious. If these should be uncovered, this can happen within the module PERIM or be discussed during the kick-off on a smaller scale.

#### **Precondition:**

In order to be able to perform a test, the SySS GmbH always requires a written declaration of consent of each respective licensee. Therefore, they have to be included when planning the test. Out of judicial reasons other ways of proceeding are not possible.

In order to be able to create the test efficiently, third parties should also provide a contact person for further enquiries. If the examination of their systems is the main part of a test, the preconditions for each module apply for third parties in the same way.

It has to be clarified during the kick-off, who the person is to be informed about the test and whether the report has to be divided up and how many copies are needed.

#### **Tips by Sebastian Schreiber:**

A high security level is the basis for confidence in the products of your service provider. Inform him that you offer him to have his security level checked by the SySS GmbH and to bear the costs.

Check at all times whether third parties are concerned. Get their written declaration of consent in time. Third parties should not be confronted with test results unprepared as you need their cooperation for remedying vulnerabilities.

If you want to simplify such processes, include the authorization for performing security tests in the Service Level Agreement.

## 4.2. Forensic Analyses (FORENSIC)

Any kind of security incident has to be analysed in detail in order to be able to obtain a conclusion about the procedure and even about the perpetrator, if possible. The SySS GmbH can give support by supplying forensic analyses.

They can be performed in several variations. On the one hand the compromised system can be analysed directly – the proceeding is conform to a test at a laboratory. The affected system may be allocated to the SySS GmbH or analysed directly on-site.

On the other hand forensic science may take place supporting internal measures by evaluating log files and by actively analysing an affected system for security holes.

### **Customer's Assistance:**

It goes without saying that a contact person needs to be at hand for such analyses, who knows circumstances, has certain background information and can establish contact to the actual users.

Furthermore, the way how the forensic analysis is to take place has to be discussed. The SySS GmbH cannot prepare the project effectively if extremely precise information about the object to be tested, i.e. technical details of the hard- and software to be tested and the organisational structure, are not at hand. If any of those results of the project should be able to be processed in a legal way, respective institutions like the legal department have to be informed as early as possible so that they also have sufficient time for any necessary researches.

### **Tip by Sebastian Schreiber:**

From all tests offered, forensic analyses are the most individual projects which my company conducts. Therefore, take enough time for a detailed preliminary talk!

When facing your first “case”, above all things keep calm and carefully talk the issue through with my members of staff. Technical measures without having a clear situation can easily lead forensic analyses in a wrong direction and extend the project unnecessarily. The time invested in preparing and clarifying the issue has a direct influence on the quality of the analysis result.

Avoid premature conclusions (like, for instance, an early naming of guilty persons). Forensic artefacts can have several meanings both in the IT and in other areas of expertise. On their own, they are normally not of great value (e.g. without the information who has the right to access a certain building and who has not or who is assigned a particular system).

### **4.3. Check of Organisational Requirements: REVIEW**

#### **Starting Position:**

When considering IT security as a process, it cannot be warranted by purely selective measures. Therefore, the SySS GmbH offers analyses of the organisational requirements defining IT security. These are security policies, security handbooks but also standard settings within the IT infrastructure. When doing a review, the material to be analyzed is made available for our consultants who in return have to get familiar with it and will eventually recommend improvements and alterations. By request, reviews can also be done or accompanied by conversations or workshops. This module covers the non-technical analyses within the frame of security tests but cannot stand on its own. In order to control the status of the actual implementation of requirements or a security policy, we recommend choosing a suitable test module.

#### **Preconditions:**

When performing reviews, the SySS GmbH requires the current versions of the material to be checked. There are a number of incidents which can easily lead to the fact that the respective requirements of the situation described is not conform to the real one anymore. Indications to this can only be made by members of staff of the customer company. Therefore, this module can not be executed without a contact person from customer’s side who should be available to answer any questions or mediate the contact to respective persons in charge.

#### **4.4. Individual Issues: INDIVIDUAL**

In case it is not possible to cover your issue with the modules presented in this paper, please do not hesitate to get in touch with us on the phone and to expound it to us. In next to all cases we will find a solution together as we possess longstanding experience and expertise in nearly all areas of IT security consultancy.

## **5. Basics of Security Tests**

A security test is performed in order to detect any kind of security flaws and to remedy them afterwards. In the case of a test by the SySS GmbH, SySS detect them and the customer does the remedy.

### **5.1. Limitations of Security Tests**

A security test analyses the present state of the computer system. It is very difficult to realize risks emanating from possible configuration changes or new facts in the future. Such considerations always have a speculative character. Security tests only have an impact if they are performed on a regular basis.

Detected vulnerabilities are also dependent on the test perspective. When doing a test according to the module INTERNET, local weak passwords are not discovered, for instance, if there is no possibility at all to log on to the system to be tested from the Internet.

Another problem is a tight budget: If big networks or complex web applications are tested in only a short time, there is the danger that security holes may not be identified, utterly out of a lack of time. A potential perpetrator taking sufficient time for a more profound analysis may be able to detect and exploit security holes.

The main focus when performing security tests is primarily on the identification of vulnerabilities being – at the time of the test – a high, concrete risk. Therefore, it is especially efficient in this area.

## **5.2. Comparison between Security Tests and other Examinations**

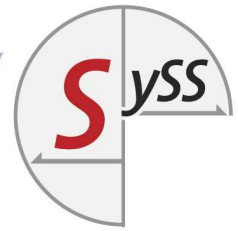
Compared to IT basic protection audits and certificates according to ISO 27001, a security test is more detailed, creating checkable facts and naming direct threats for the IT security.

Security holes can also be proven if BSI certified software is used and if an ISO 27001 certificate is at hand. Therefore, autonomous security tests being performed by specialists are to be preferred to security examinations within the frame of respective audits.

They do not compete with such measures but are rather ideal as a support – especially as there may be comparably quick results and as they can be integrated into an existing audit.

## **5.3. Ten Tips by Sebastian Schreiber:**

1. Perform security tests on a regular basis, e.g. once a year.
2. Focus especially on the test of web applications.
3. Define the time frames for penetration tests early.
4. Take care that contact persons of your company may be available within these time periods.
5. The quality of security tests mainly depends on the quality of the information exchange between service provider and customer. Your contact person should therefore be named early and be well informed.
6. Assure yourself of the quality of work of the penetration tester by seeing him/her and attending the test for one or two days. Invite other persons concerned (your boss, service providers, colleagues, etc.) to do so, too.
7. Unannounced tests are counter-productive as they rather evoke your colleagues' mistrust instead of confidence.
8. Choose the systems to be tested for internal tests very carefully and be prepared for breakdowns.
9. Organisational preparation of the test pans out: Take enough time for the kick-off.



10. Only commission specialists with security tests. Superficial tests only attest pretended security.

## **6. About the SySS GmbH**

### **6.1. The Company's History**

The SySS GmbH was founded in 1998 by Sebastian Schreiber, a graduate computer scientist, in order to offer high-quality security tests. At present, the SySS GmbH employs 29 members of staff of whom 18 exclusively perform security tests.

The customers of the SySS GmbH are companies of different branches and sizes. Among them are, for instance, HEWLETT-PACKARD, IBM, ROBERT BOSCH GMBH, KODAK, the EUROPEAN COMMISSION, UNION INVESTMENT, SCHUFA, SAP, INA, T-SYSTEMS, RENAULT-NISSAN BANK, DEUTSCHE FLUGSICHERUNG, OCE, BUNDESWEHR, DAIMLER AG, MÜNCHENER RÜCK, INNENMINISTERIUM/LKA NIEDERSACHSEN, THE EUROPEAN CENTRAL BANK, FESTO AG, BURDA SYSTEMS, DEUTSCHE BANK, and so on. You will find more reference customers on the homepage of the SySS GmbH.

Sebastian Schreiber, the SySS GmbH's managing director, and other members of staff regularly give lectures on national and international congresses in cities like Belgrade, Berlin, Bratislava, Bucharest, Budapest, Dublin, Helsinki, Kiev, Las Vegas, Lisbon, Ljubljana, London, Moscow, Paris, Prague, Riga, Stockholm, Vienna and Zagreb, for instance.

Besides, they also regularly publish articles in a number of specialist journals and print media such as SPIEGEL, Stuttgarter Zeitung, Züricher Zeitung, etc... The SySS GmbH is also present on television.

### **6.2. The Special Way to Proceed**

#### **Specialization:**

The SySS GmbH is specialized on security tests and offers a range of trainings in this field. This extremely high level of specialization enlarges the wealth of experience of all consultants, which is further extended by the regular performance of security tests.

Therefore, the SySS GmbH knows the needs of their customers very well and are thus able to deliver a precise result of the test. It offers a critical but fair external perspective on the security level.

Counselling services for remedying acknowledged security holes are only necessary to a minimal extent – our customers are very successful in putting any necessary remedial measures into practice themselves.

### **Transparency:**

The SySS GmbH finds it highly important that the customer can comprehend without further ado how vulnerabilities are recognized and get exploited within the frame of the test. If hacking is understood as a mysterious, strange matter, it does harm to the strength of the security within the company.

Transparency can be achieved by observing the following points:

- Within the module DOCU, high-quality documentation will be compiled whose aim it is that security holes can be comprehended.
- It is helpful if the customer invites all its members of staff concerned to either attend the security tests fully or partially. The SySS GmbH is willing at all times to serve the customer with its knowledge.
- Presentation of the result (module PRES) by the consultant, who has led the test.

Only by showing such openness, a positive perception of security tests can be achieved among the customer company's members of staff.

### **Flexibility:**

When performing tests, the SySS GmbH does not follow a set pattern but is flexible. A fix pattern would be misconceiving the nature of an attack as every network is different and every step during a test is dependent on the preceding.

Additionally, it is possible to change the main focus during a test by direct communication between the contact person and the consultant in charge.

### **Quality Assurance:**

The quality assurance of the reports, which are being processed within the module DOCU, is always issued by a further experienced consultant. Thus, the comprehensibility of test results can be ensured. If possible, we try to achieve as much QA as possible during a test already. Furthermore we also make sure that the reports are proof-read for spelling mistakes and comprehensibility. This is done by our in-house lector.

### **6.3. Tools**

Both the entire proceeding of a test and the choice of tools are part of the leading consultant's responsibility. He/she adjusts the course of the test to the test object and especially to the test depth on the basis of his/her experience and chooses the optimal tools.

Therefore, the following overview is just a choice of tools, which are generally used within the modules INTERNET and LAN/WAN:

- In order to detect systems and services, port scanners like NMAP, UNICORNSCAN or WOLPERTINGER are used.
- Automated vulnerability scanners we use are NESSUS, SAINT and MAXPATROL
- In order to exploit found vulnerabilities, we leverage tools like the METASPLOIT FRAMEWORK, CORE IMPACT or IMMUNITY CANVAS
- For the further examinations of odd services, there is a high number of tools on hand like, for instance: RELAYSCANNER, SMTPMAP/SMTPSCAN, IKE-SCAN, DNSWALK and the HPING family.
- Manual checks are supported by TELNET, NETCAT, SOCAT, CRYPTCAT, OPENSSL and STUNNEL.

Concerning web application tests we use proxy tools like the BURP SUITE PROFESSIONAL, the CHARLES PROXY or WEBSCARAB.

In order to test WLAN, the SySS GmbH preferably uses KISMET, the AIRCRACK-NG family, a highly customized version of KARMA, NETSTUMBLER, HOSTAPD and AIRJACK.

The expected gain of insight on the one hand and the test depth on the other are the basis on which the consultant decides which tools to use. Not every tool is suitable for every kind

of software. The use of every tool has a certain minimum duration – if this extends the time frame of the test considerably, the tool can not be used.

If the scheduled time frame of the test allows, tools may be used which have been published only after the start of the test.

#### 6.4. Fundamental Ethics for Penetration Testers

On the basis of already existing codices and experiences made over the years, the SySS GmbH has made an advance to issue a fundamental code of ethics for penetration testers. This code was first published in the German periodical *Datenschutz und Datensicherheit*, issue 04/2009 and reflects the attitude and the basis on which the SySS GmbH works. Therefore, we work according to the pattern of the following code of ethics:

- **Independence:** Companies performing penetration tests only test in enterprises in which they have neither taken part in planning the IT environment nor in the implementation of any security measurements. Furthermore, they also abstain from testing companies they have sold their own software to or want to sell software to. This is the only way to safeguard that test results are impartial.
- **Confidentiality:** Both the identity of the commissioning company and any insights into internal networks, structures and respective data including those having been allocated to the penetration tester are to be treated with absolute confidentiality.
- **Prohibition of Commission Fees:** Accepting any kind of monetary commissions or other comparable advantages is interdicted.
- **Care:** The customer is to be informed about any possible risks which can emanate from the tests.
- **Professionalism and Quality Assurance:** All work has to be done in a professional way and to undergo a quality assurance. A penetration tester does his work to the best of his technical knowledge.
- **Liability:** Any consents agreed both by contract and orally in counselling interviews are to be adhered to by the members of staff of the company performing penetration tests and are binding.
- **Impartiality, Neutrality and Transparency:** Conclusions must be impartial and to be depicted in a comprehensible way.

- **Conflicts of Interest:** Conflicts of interest between penetration testers and customers are to be avoided and if so reported and smoothed out.
- **.Strict Obedience of Laws:** The laws of the country where the penetration test is performed are to be kept strictly even if partial results of a penetration test could in itself be a conflict of interest with the existing legislation. Thus, the discovery of vulnerabilities in certain cases can promote breaches of law. Penetration testers therefore are bound to make them acquainted with the respective legal situation and to carefully take heed to their work being done within the existing legal boundaries.
- **Respect of Human Beings:** *Social Engineering* attacks are directed at the behaviour of human beings. Therefore they will only be performed – if they happen at all – with prior notice.
- **Quoting Correctly:** If knowledge from outside is considered and used during the course of work, sources and authors have to be indicated to in a correct way.

## 6.5. Description of Technical Risks during Tests

### Load when Testing Web Applications

Performing security tests is similar to functional tests; loads will be generated on the data base powering the web application. This can happen by a search via all fields which apparently a normal user of the application cannot perform. If the system on which the data base is running is calculated in a very tight way, there can be disturbances. Therefore, a manual administration of the data base by members of staff of the customer company is necessary. From an external perspective, only the frequency of search requests can be altered but not the priority of one search compared with another.

### E-Mails to Internal Addresses

Certain functionalities enable e-mails to be sent via web applications, e.g. when requesting products. These functionalities must neither be able to be used for spam mailing nor be abused for faking e-mails. Problems in this case occur nearly without exception by the systems involved in the mail order, which are not capable of dealing with a series of automatically created messages. Also here, the manual care for all systems involved is

necessary as from an external point of view, it is only possible to vaguely suggest how all systems involved are put together.

The SySS GmbH therefore recommends that such systems should not be designed for an extremely low volume for utilization but to provide sufficient power reserve. Such reserve can also be gained by optimizing the data base and the search engines of the web applications.

When using old systems, however, a load reduction by optimizing the data base will have its limits.

### **Breakdown of Infrastructural Components**

Security tests create a certain network traffic, which the components involved, the router and the switches, have to operate. They are expected to work as correctly as when operating regularly. Any load occurring during a security test naturally complies with the load being created by a very intensive use of numerous communication services. Infrastructural components, which break down during such tests instead of becoming slower are to be seen extremely critically. Even when the load is higher than during its legitimate use, the load of a security test can not compete even rudimentarily with that of a spread out attack (*DDoS*). Furthermore, there is the risk that the systems can not quench naturally occurring load peaks either.

Normally, such occurrences can clearly be traced back to the hardware in use and its running software. If software is not supported by its producers anymore, the SySS GmbH strongly recommends an upgrade. The risk can further be reduced by a slower test procedure which, however, can easily multiply the time needed for the project.

### **Insufficient Wire Capacity**

The SySS GmbH mainly use root servers for tests in the Internet. Both the systems and the used tools themselves are available for everyone. At the time of writing this section for the white paper, approximately two dozen private broadband connections had the same sending capacity as one root server. Therefore, the necessary load during a security assessment can also be created by third parties with only a very little financial expense. This means that in reality practically every broadband connection would be capable to overload a 2 M/bit track or at least to massively disturb it.

There is only one other factor besides the wire capacity which is determining and this is time. A reduction of the necessary bandwidth can only happen when the test period is longer. The only alternative are samples.

As the wire capacity cannot be estimated precisely from an external point of view, the SySS GmbH is therefore dependent on accurate information from customer's side. Only thus, measurements can be taken beforehand to reduce the necessary bandwidth.

In this matter, the SySS GmbH does not have any insight into contracts or other agreements of the customer and their providers and therefore cannot provide this piece of information.

The SySS GmbH recommends in general that the wire capacity is adjusted to modern demands. If one 2 m/bit line sustains several Class-C nets, for instance, disturbances will already arise from the insufficient bandwidth.

On the other hand, costs can be reduced by having some systems hosted externally, either entirely or in parts.

If this is not possible as, for instance, connections with the necessary capacity cannot be implemented locally for a reasonable price, the SySS GmbH advises to set up a clear concept in case the connection is overloaded by accident and without any mischief implied and thus cannot be used on a daily basis anymore. The contact person of the customer company should in this case always be the respective provider.

## 6.6. Publications of the SySS GmbH (Samples)

The SySS GmbH regularly publishes articles in journals or papers at congresses. Most of them are published in German but a few publications are also in English. This list of publications will first list the English publications and then the German ones.

### Publications in English:

Deeg, Matthias: *SySS Cracks Yet Another USB Flash Drive*, SySS Publication, [www.syss.de](http://www.syss.de), 02/2011

Deeg, Matthias: *Privilege Escalation via Anti-Virus Software*, SySS Publication, [www.syss.de](http://www.syss.de), 01/2011

Eichelmann, Christian: *SySS Spies Out Data on iPhones*, SySS Publication, [www.syss.de](http://www.syss.de), 02/2010

Deeg, Matthias: *SySS Cracks Hardware-Encrypted USB Flash Drive from SanDisk*, SySS Publication, [www.syss.de](http://www.syss.de), 12/2009

Schreiber, Sebastian: *Concept of a Professional Code of Ethics for Penetration Testers* (transl of a German article *Entwurf einer Ethik für Penetrationstester*), Datenschutz und Datensicherheit, 04/2009, see [www.syss.de](http://www.syss.de)

### Publications in German:

Deeg, Matthias: *SySS knackt weiteren USB-Stick*, SySS Publikation, [www.syss.de](http://www.syss.de), 02/2011

Deeg, Matthias: *Rechteausweitung mittels Antivirensoftware*, SySS Publikation, [www.syss.de](http://www.syss.de), 01/2011

Borrmann, Micha: *Kurze Sicherheitsanalyse von OWOK light*, SySS Publikation, [www.syss.de](http://www.syss.de), 01/2011

Bott, Christoph/Schreiber, Sebastian: *Bedroht „Hole 196“ die WLAN-Security?* in: VAF Report, Ausgabe 03/2010

Deeg, Matthias/Eichelmann, Christian: *Angriff auf Online-Banking-Applikation*, SySS Publikation, [www.syss.de](http://www.syss.de), 03/2010

Eichelmann, Christian: *SySS späht Daten auf iPhones aus*, SySS Publikation, [www.syss.de](http://www.syss.de), 02/2010

Schreiber, Sebastian: *Rechtliche Aspekte von Penetrationstests* in: Wirtschaftsinformatik und Management (WuM), 01/2010

Schreiber, Sebastian: *Totgesagte leben länger* in: KES 4/2009 – antithesis to Brian Chess' statement that penetration tests would die out.

Schreiber, Sebastian: *Vorschlag zum Entwurf einer Berufsethik für Penetrationstester* in DuD (Datenschutz und Datensicherheit) 04/2009

Muncan, Michael/Schreiber, Sebastian: *Interne Penetrationstests – Sicherheitstests im Firmennetz* in DuD 04/2009

Arbeiter, Stefan/Deeg, Matthias: *Bunte Rechenknechte* in: C't 6/2009

Borrmann, Bachfeld: *Zechpreller: Unsichere Bezahlungssysteme* in C't 6/2008

Heinrich, Katrin/Schreiber, Sebastian: *Penetrationstests als Instrument der Qualitätssicherung* in IT Sicherheit und Datenschutz 6/2007

Bott, Christoph/Schreiber, Sebastian: *Penetrationstests – Hackerangriffe als Kontrollinstrument* in: S&I April 2007

Borrmann, Micha/Schreiber, Sebastian: *Sicherheit von Web-Applikationen aus Sicht eines Angreifers* in: DuD -Datenschutz und Datensicherheit, 11/2006

Schreiber, Sebastian: *Suchmaschinen als Hackerwerkzeug* in: PC-Magazin 7/2006

Schreiber, Sebastian: *Securitykosten am Beispiel von Penetrationstests* in: Praxis der Wirtschaftsinformatik, April 2006

Schreiber, Sebastian: *Google Hacks – penetrante Suchmaschinen* in: KES 4/2005

Schreiber, Sebastian: *Hackertools und Penetrationstests* in: HMD 236 - Praxis der Wirtschaftsinformatik, Ausgabe v. 23.4.2004

Kroma, Pierre/Schreiber, Sebastian: *Störfunk - D.o.S. gegen WLANs* in: Heise Security, Ausgabe v. 12.03.2004

Borrmann, Micha/Schreiber, Sebastian: *Wer zählt, gewinnt* in: C't 23/2003, S. 212

Borrmann, Micha: *Unentdeckt Ports scannen* in: Network Computing 10-11/2003, S.46

Schreiber, Sebastian: *Ans Licht gebracht* in: Kommune21 6/2003, S.34f.

If you are interested, we are very happy to send you our press file containing all kinds of different articles from members of staff of and articles about the SySS GmbH.