

Modular Project Process Plan for a **Security Assessment** by SySS.

1	General information on project structure.....	2
1.1	Advantages of penetration tests.....	2
1.2	Analytic techniques	2
1.3	Structural parameters of penetration tests	2
2	Modular project process plan	3
2.1	Zero-knowledge test: ZK (1.5 MD).....	4
2.2	Kick-Off: KICK (0-1 MD)	4
2.3	Conducting analysis online: INTERNET (as a rule 2-10 MD)	5
2.4	Security assessment of the corporate network: CN (ca. 2-10 MD).....	6
2.5	Testing a web application: WEB (2-4 MD per application).....	6
2.6	WLAN test: WLAN (1-2 MD)	7
2.7	Analysis of documents: REVIEW (1.5 MD).....	7
2.8	Interviewing key employees: INTERVIEW (2 MD)	8
2.9	Traffic analysis: TRAFFIC (1 MD)	8
2.10	Compiling documentation: DOCU (1-4 MD)	8
2.11	Presentation workshop: “Results & measures”: PRES (1 MD)	9
2.12	Conducting backup test: BACKUP TEST (0.5-2 MD).....	9
3	Specifics of the SySS approach.....	10
4	References for SySS	10
5	Publications by SySS.....	10
6	Legal framework	11
7	Annex	11

1 General information on project structure

The goal of a security assessment is to identify security weak points in the customer's IT infrastructure.

1.1 Advantages of penetration tests

A penetration test is the only way to identify, rapidly and with little effort, weak points in complex networks. Experienced professionals carry out attacks from the hacker's perspective. The customer is enabled to react quickly to systemic flaws.

1.2 Analytic techniques

In identifying security gaps, a large number of completely different techniques are available:



1.3 Structural parameters of penetration tests

Penetration tests can, depending on the customer's needs, be set up in completely disparate ways. The following structural parameters are defined in liaison with the customer:

- **Current knowledge**

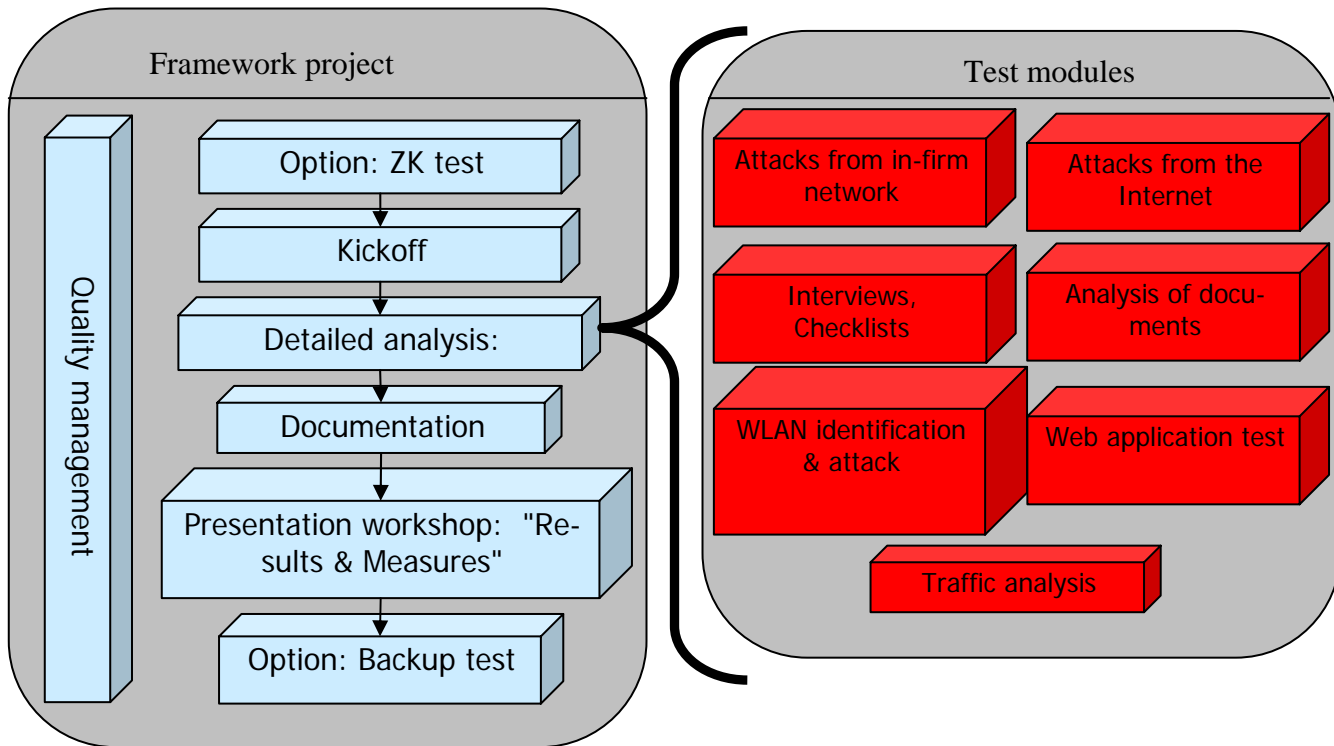
- Zero-knowledge test
- White box test
- **Simulated source of attack**
 - from the Internet
 - from the company's own network
- **Aggressiveness**
 - Are D.o.S. attacks included?
 - A certain residual risk of impairments should be deemed acceptable.
- **Means of attack**
 - Purely technical methods
 - Social engineering
 - Analysis of documents
 - Interviews
- **Profundity of test**
 - Rough-and-ready testing of many systems
 - Careful and comprehensive testing of particularly critical systems
- **Announced/unannounced:**

	Announced	Unannounced
Advantages	<ul style="list-style-type: none"> ● Generates security awareness ● Cooperative approach simplifies testing and choice of measures 	<ul style="list-style-type: none"> ● Unfalsified assessment possible
Disadvantages	<ul style="list-style-type: none"> ● Slightly falsified picture cannot be ruled out 	<ul style="list-style-type: none"> ● Generates mistrust ● Administrator feels sidelined ● Undesirable reactions possible

- **Evading IDS**
Other than with so-called “noisy scans”, attempts can also be made to carry out undetected attacks. Logfile entries and/or alarms by IDS can thus be avoided.

2 Modular project process plan

Penetration test projects invariably follow the same scheme. They consist of a framework project and various elective test modules. According to the customer's security needs and the complexity of the infrastructure to be tested, the amount of time budgeted can vary enormously. Thus, a lean project might take no more than two man days, while a comprehensive project could easily take several weeks.



2.1 Zero-knowledge test: ZK (1.5 MD)

At the customer's request, an attack from the outside can be launched as part of a zero-knowledge test (i.e. without any prior knowledge). Here we receive no information whatsoever from the customer. Using databases available online, the first step is to analyze by which access pathways/IP addresses the company to be tested is linked to the Internet.

The data ascertained by us will be communicated to the customer's designated project handler. If during the course of the project we receive information from the customer, we will document this with a timestamp.

Procuring information:

A list of IP addresses belonging to the customer will be compiled. Routers for the ISP or extraneous systems used by the customer (DNS, email, www,...) will also be included. Creative thinking is applied to acquire as much information as possible about the actual infrastructure:

- Mail routing
- DNS infrastructure
- Cross-firm communication links
- Networking with branches
- Identifying subsidiaries
- Searching in mailing list archives/newsgroups
- Other possibilities

The systems identified by us will be communicated to the contact person; any non-identified systems will be supplemented by the customer.

2.2 Kick-Off: KICK (0-1 MD)

A preliminary discussion (e.g. by phone) will be held to specify in detail how the assessment will be carried out. Issues to be defined are:

- by what techniques will security critical problems be identified
- how aggressive the attacks should be (with the prospect of the systems being brought down in case of a success)
- contact persons for the project
- the infrastructure to be tested according to the wishes of the customer

2.3 Conducting analysis online: INTERNET (as a rule 2-10 MD)

The test involves trying to break in via the Internet to the systems being tested.

In our testing we use three sorts of methods:

- Using a security scanner (e.g. Nessus, ISS, or NetRecon)
- Portscan with the powerful Open Source Portscanner Nmap
- Manual tests (hacking) using self-developed software and techniques.

Security scanners are only used to speed up our work. However, the real value of our work lies in the manual tests:

We verify the scanning result and attempt to identify current security weaknesses that have eluded the scanners. In fact, experience shows that approximately 75% of systems compromised during a test can be defeated only by experience, imagination, and human intelligence.

The following points are included in the test:

- Checking the software used by the servers for security flaws
- Attacks by guessing the passwords
- Portscans with non-RFC compliant packages (SYNscan, ACKscan, FINscan and Xmasscan), by means of which firewalls (e.g. static package filters) might conceivably be overcome
- Identifying the operating systems and software used.
- Targeted checking of individual services using hacker software as well as our own software
- Analyzing the SNMP servicing capability of routers and other network components
- Checking the DNS server and the email server (focusing on current vulnerabilities of widely used DNS software)
- At request, aggressive scans can additionally be performed - both those in which there is only a risk of the system crashing and those whose goal is to crash the system in question
- Identifying open relays, old DNS versions, inadequately patched MS-IIS servers, and vulnerable CGI scripts, etc.
- Use of the latest "exploits" and hacker tools from the Internet

This test may be conducted blind, i.e. our security experts receive no insider information whatever; all they are given to check is a domain name or a list of IP addresses.

IDS test:

During testing, the customer can observe the logfiles of the IDS, thus ascertaining to what extent our attacks/scans have an impact on the log file. At request, we can disguise our attacks using stealth technologies (“IDS evading”).

2.4 Security assessment of the corporate network: CN (ca. 2-10 MD)

Security tests are also performed from the Intranet: the same test methods are deployed, with the exception of attack methods that only work with firewalls.

Still, an internal test differs considerably from an external one. While only a bare minimum of company computers can be accessed from the Internet, and even these are protected by a firewall, normally all computers have no defences against being attacked from the Intranet. The pool of potential in-house attackers is, however, smaller. In large companies, there are often very many identically configured systems, of which only one representative per system is scanned.

Password audits:

At the customer’s request, the passwords used can be submitted to a quality control. We operate with test techniques belonging to classes A-D:

	Dictionary Attack	Letter- or syllable- oriented attacks
Cracking password hashes (e.g. from Windows SAM file)	A	B
Attacks at protocol level	C	D

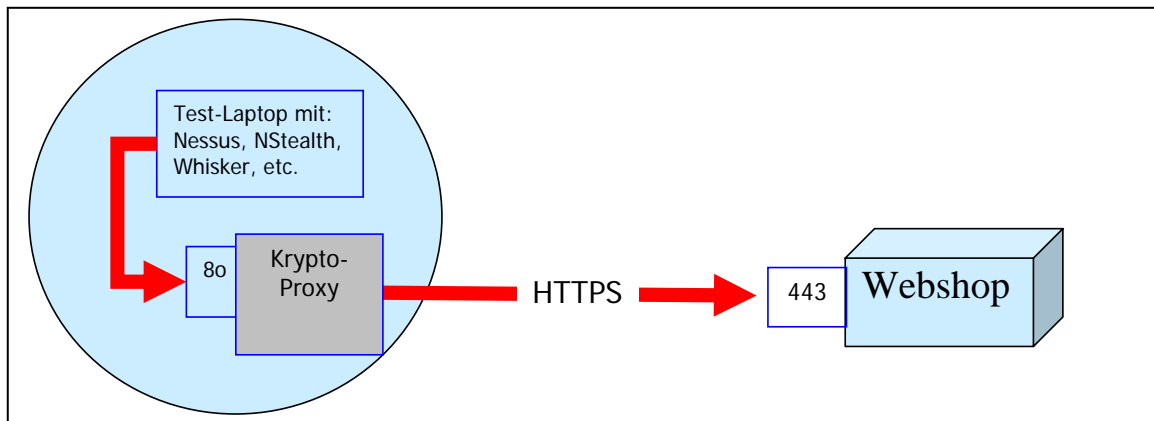
2.5 Testing a web application: WEB (2-4 MD per application)

Attacks on web applications are, by definition, very demanding. Since these are mostly individual solutions, experience and imagination are required. Automated scanners are not suitable for testing such applications. SySS has tested web applications from a variety of sectors (banks, insurance companies, TK providers, and a number of web shops). Experience has invariably shown that developers of web solutions pay far too little attention to IT security. Outside sessions can often be “hijacked” or directories can be spied on using metacharacter attacks,.

Web servers available on the market (Apache, IIS, Domino, IPlanet, Websphere, etc.) often themselves have weak points or are inadequately configured.

The test requires two normal user access ways, via which we try to penetrate protected areas. Here the http communication setup is closely analyzed and checked for weak points. The following attack works regularly: The attacker logs in as user A and is able, by skillful URL manipulation, to inspect data belonging to other users.

Deploying our own techniques, this can even work for SSL/HTTPS connections:



2.6 WLAN test: WLAN (1-2 MD)

WLANs are user-friendly and not too expensive. It is commonplace to have the so-called “wild” WLANs installed without the IT department knowing. As part of the test module, the customer’s WLANs are identified. It is tested whether effective access control (authentication) is being performed and whether encoding and access control are correctly configured. Any operant extensions to IEEE 802.11b (such as Cisco’s LEAP) are recognized and assessed.

SySS operates a test van equipped for what is known as “war driving”, thus enabling the WLANs to be tested even on large corporate sites.



2.7 Analysis of documents: REVIEW (1.5 MD)

The customer presents his own infrastructure using a network plan. The security weak points and the need for optimising certain aspects of system security are discussed.

In addition, existing documents are analyzed in this project segment. This should include (if available) the following documents:

- Security plan
- Security guidelines and policies

- QM manual, documentation of in-house processes
- Organization charts
- Documents relating to IT systems:
 - Firewalls
 - Intrusion detection systems (IDS)
- Any other relevant documentation

2.8 Interviewing key employees: INTERVIEW (2 MD)

Practice shows that informal processes, not documented anywhere, exist within companies. Also, employees are often very well aware of weak points and about where improvements are possible. Interviews are held to ascertain what employees know and to evaluate this. As a rule, ca. 7 employees should be interviewed. Each interview lasts about 50 minutes. The series of questions we use has been tested in a large number of projects. It is best to recruit interviewees from a variety of departments. Long standing employees are particularly suitable.

2.9 Traffic analysis: TRAFFIC (1 MD)

Internal networks make use of a variety of protocols. Traffic analysis tries to determine which protocols are in use and which data flows exist. In our report we highlight especially the protocols that transport uncoded user data and passwords.

2.10 Compiling documentation: DOCU (1-4 MD)

Each step is documented in detail. This is an important aspect of quality management. Documentation can be between 20 and 1,000 pages long and cover the following points:

- All protocols and log files created during the tests
- The results of the security scanners used
- Non-technical presentation of results (“executive summary”)
- PPT presentation (if requested)
- Own analyses
- Theoretical considerations/leads
- Assessments

If the documentation runs to more than 1,000 pages, only the executive summary will be made available in print. The complete documentation (including all analysis protocols) will be delivered in electronic form (CD-ROM or coded email).

The unambiguous CVE-ID will be supplied with the identified security weaknesses (see also <http://cve.mitre.org>). This CVE-ID will enable the customer to compare results tabulated by various consulting companies in the security sector. If the security weak points are so new that no CVE-IDs exist as yet, we will use Bugtraq IDs instead.

In addition we will, together with the customer, compile analysis setting out recommendations for future security development.

The core points of the assessment are summarized in an *executive summary*. All weak points are itemized, commented, and assessed. Counter measures are proposed for all security weak points. The last item - Action - will, with the customer’s assistance, be filled out at the presentation. The scale, the timing, and the personnel in responsible for

implementation of the proposed measure will be defined. The *executive summary* might therefore look like the following:

Heading	Explanation	Proposed measures	Risk	Action
				Person responsible
				Day of test
ProFTPD for ftp.firma.de	The installed ProFTPD FTP server has a series of security weak points.	Migration to a safe FTP server dispensing with the unsafe FTP protocol		Migration
				Mr. Schmid
				March 1, 2003
IIS/dvwsr.dll	A security gap in this DLL permits access by unauthorized parties. Affected are the banking.firma.de and www.firma.de systems.	De-install Office 2000 server extensions or FrontPage 2000 server extensions		De-activate FP extension
				Mr. Maier
				February 1, 2003
Bind/DNS	Antiquated version of the name server software BIND is in use. These versions are exposed to a variety of attacks.	Update to a new version of BIND. "Recursive queries" should not be allowed.		none
In-firm process	Unauthorized persons can have passwords changed by phone.	Securing the process (see below)		none
DNS zone transfer	Any computer can perform zone transfers.	Restricting rights of access		none

Documentation is forwarded either by coded email or by normal mail (recorded signed for delivery).

2.11 Presentation workshop: "Results & measures": PRES (1 MD)

A workshop will be held to discuss the results of the security assessment with the customer in terms of the documentation compiled in the DOCU step. The catalogue of measures together with the possible solutions are presented and discussed. The last item of the *executive summary* is completed together with the customer.

2.12 Conducting backup test: BACKUP TEST (0.5-2 MD)

Following receipt of the catalogue of measures (or during *Presentation workshop: Results & measures*) the customer will decide which of the proposed measures should actually be implemented. Following implementation (approx. 2 weeks after receipt of documentation) the implementation will be checked for effectiveness.

3 Specifics of the SySS approach

Specialization

Identifying security weak points is the only area covered by SySS GmbH.

Openness

Hacking has the reputation of being something mysterious, something not readily grasped by non-specialists. The SySS approach aims at achieving the opposite: We are committed to demystifying the whole process. This is why the detailed way in which we proceed and the transparent presentation of the results are an essential part of the documentation process. The customer is encouraged to be present at penetration tests and to ask questions, the idea being to enable transfer of know-how to the customer.

Focus on teamwork

Even in small and midsize companies there are heterogeneous networks: A large number of products and protocols are in use. To assure that we do not overlook any flaws, the security tests are often performed by a team of consultants.

4 References for SySS

Thanks to our highly specialized approach, many companies trust in the quality of the work we do. Our customers include: HP, IBM, Bosch, Siemens, The European Commission, Union Investment, Defense AG, DocMorris, Grundig AG, Walter AG, Paul Hartmann AG, INA Wälzlager, Elaxy AG, Allasso/Integralis, Behr, DisCON, DeTeWe, I.CON Systems, NCP, Netstuff, TÜV München, T-Systems, SerCon, Intra2Net AG, ESB Rechtsanwälte, DSD, Renault-Nissan-Bank, Deutsche Flugsicherung, Burda, Wüstenrot, Württembergische Bank; Océ, Bundeswehr, SAP AG, Daimler-Chrysler AG, Transtec AG, Münchener Rück, Innenministerium/LKA Niedersachsen, MLP AG, Zeppelin Baumaschinen, Gambro, KDVZ Neuss, Gebr. Heller Maschinenfabrik, Ärztekammer Niedersachsen, Bock Kältetechnik, Europäische Zentralbank, GITS AG, GGB-Beratungsgruppe GmbH, Alldos GmbH, Festo AG, Land Salzburg, Burda Systems, Target Partners München, Largenet, Roland-Rechtsschutz, Deutsche Bank.

Upon request, we will be happy to pass on the names of contact persons for any of these firms.

5 Publications by SySS

SySS regularly publishes articles in professional journals and gives papers at conferences. During 2002, for example, the following articles appeared in professional journals, as did a large number of conference papers:

„Security-Tipp“ Network World 09/2002, by Sebastian Schreiber.

„Gefährliche Blockade“, C't 26/2001 by Sebastian Schreiber and Jürgen Schmidt,

<http://www.heise.de/ct/01/26/038>

„Keine harte Nuss“, Notes Magazin 1/2002 by Sebastian Schreiber

„Virtueller Ladendiebstahl“ C't 26/2002, S.92f by Sebastian Schreiber

Should you be interested, we will be happy to provide you with our press folder (effective Feb. 2003: 40 pieces) containing articles by and about SySS.

6 Legal framework

Confidentiality: All information obtained in the course of our activities will be treated with the utmost confidentiality.

Liability: We would like to point out that a security scan is a controlled attack and can affect the functionality of your systems. SySS GmbH accepts no liability for any damage caused by the security scan.

Contact person: The customer is asked to name a project handler prior to project commencement in order to better assure efficient realization of the project as well as an adequate flow of information.

7 Annex

Comments on large networks:

Checking large networks (e.g. a sub-network belonging to class B) can be very time-consuming, especially when there are Internet accessible computers that do not respond to pings and the firewall does not at all respond to attempts to establish connections to closed ports (“*dropping*”). However, we also have at our disposal self-created tools suitable for scanning even very large networks (>5,000 computers).

Automated blocking:

We assume that the customer does not react to our attacks by blocking our IP address, as doing so would falsify our results. We do not resort to any measures whatsoever designed to disguise our attacks. Automated reactions to attempted attacks are, in any case, a questionable measure (see our article C’t: <http://www.heise.de/ct/01/26/038>).

Parallelization potentials:

It is not likely to have much time left before a firewall or an eCommerce application can be produced. The duration of the security test can be minimized when several experts are deployed. How great the parallelization potentials are can be ascertained from the actual project plan.

Tools used

Penetration tests use a large number of different tools, depending on project goal, test profundity, and existing IT infrastructure. Our consultants are experts in performing penetration tests. Each year they check more than a hundred systems. The individual consultants themselves choose the tools to be used. We carry out our tests using both commercially available tools and shareware freely available on the Internet. Here is a small selection of the tools we use:

Nmap, Nessus, Netcat, Nstealth, Languard, Brutus, Snmpwalk, Tcpcat, Smtscan, Icmpquery, Dsniff, Dnsspoof, Arpspoof, Ethereal, Jolt, John-the-ripper, LC4.

We also use tools from the Internet, e.g. tools available at <http://www.securityfocus.com/tools>.

We maintain a large archive (approx. 10 GB) of tools, documents, email and news files, and exploits.

In the event that no suitable tools are available for specific tests, we modify tools found on the Internet or write our own tools. When attacking the Lotus Domino webserver, we have, for example, developed our own scanner, which is superior to all scanners that are available commercially or free of charge.

For manual tests, we often write programs for single application only.