

Compass Security Assessments

Security Review & Penetration Testing



Compass Security AG
Werkstrasse 20
Postfach 2038
CH- 8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Security Reviews & Penetration Testing

Introduction

Security reviews and testing are important components of the risk management process. Potential vulnerabilities and weaknesses are traced in order to ensure that the security infrastructure is consistent with the business requirements as well as with the defined and accepted residual risks.

Facts

- ✦ Configuration weaknesses and outdated systems influence the availability and quality of a system. This can result in substantial losses.
- ✦ Effectively conducted risk management: If not sufficiently protected, the IT infrastructure may become a target for attacks.

Compass Services

Security assessments are the core competence of Compass Security. We are highly experienced in the testing of Web applications. From our point of view this becomes increasingly important with the current shifting of the weaknesses to the application level. Our procedures are based on common methodologies such as OWASP or OSSTMM.

Compass offers the following services in the field of security assessments:

- ✦ Security Reviews
- ✦ Vulnerability Scanning
- ✦ Web Application Testing
- ✦ Ethical Hacking/Penetration Testing
- ✦ Social Engineering

As a result, the customer obtains vital hints where in the system or the organisation the vulnerabilities are and which measures may be taken to improve the situation.

Compass Security pursues a modular approach. During Ethical Hacking respectively Penetration Testing an attacker is simulated who trespasses into a computer or network without authorisation. A Security Review aims at detecting configuration errors and weaknesses within complete infrastructures, systems or applications.

Procedure

First of all, the aims of an assessment and the necessary modules have to be defined together with the customer. Depending on the situation a Security Review can be more adequate than a testing, because a higher efficiency and accuracy can be achieved by the insight into the system configuration. Often both types are combined: In a first step a Security Testing is performed, which is supplemented in a second step with a targeted review of selected systems.

Another vital question is how the assessment shall be conducted.

Is the access necessary only from outside (Internet) or also from the Intranet respectively directly in the DMZ? Shall an attack be performed anonymously or as a registered user? What level of information is expected of the person conducting the test?

The more information is known, the more focussed and efficient the testing can be performed (Whitebox approach). On the other hand, with no or little information about the target system, it can be demonstrated what an attacker can find out within a certain time (Blackbox approach). Is social engineering, e.g. via telephone or by the delivery of a Trojan, permitted for the gathering of information?

The aim of a Security Assessment also outlines the depth of the respective tests. If the search for respectively the demonstration of potential weaknesses is of priority, a Security Review and/or a Vulnerability Scanning are sufficient. The Penetration Testing goes one step beyond, where it is attempted to make use of the detected weaknesses.



The following questions may be useful for the definition of an order:

- ✦ What attacks do you want to prevent?
- ✦ What has to be protected?
- ✦ Who do you want to protect from?
- ✦ Where are attacks to be expected from?

Preparation and performance

Based on the above information as well as on the number of components to be tested, the necessary expenditure of time can be estimated. Now a date for the testing has to be fixed: What kinds of investigations and preparations are necessary? Examples are the application for access rights, the creation of user accounts or the provision of a stable testing environment. Where possible, Compass Security always performs the tests with their own hard- and software.

The operator of the infrastructure to be tested must in any case be informed of the test beforehand and must agree with it (Declaration of consent). Furthermore, for the whole test period a contact person must be appointed who can react accordingly if necessary.

What is expected of the documentation? Shall it be drawn up in German or English? Is there a need to deviate from the Compass documentation structure? How widely is it spread? For quality reasons every report is cross-read by a Compass employee who did not take part in the specific project for a second opinion.

If requested the results will be presented and discussed at customer's site.

As an independent and neutral service company we do not implement the measures suggested. However, we gladly support you in checking whether, respectively how far, the situation has improved.

Security Assessments basically represent a picture of the current situation and are thus only relevant for a short time. Therefore we recommend checking an

environment respectively certain partitions specifically and regularly on their security. Security is not a stable condition but a continuously developing process. In other words: After the test is before the test!

Your advantages

- ✦ You receive a report where the weaknesses are listed and prioritised. Furthermore measures to improve the situation are proposed.
- ✦ You gain information about whether the security measures you have taken meet the common requirements.
- ✦ Based on the detailed appendix you learn how the tests have been performed and what aspects you should consider in future projects.

References

The clientele of Compass ranges over all sectors of the national and international economic environment. Due to the confidentiality towards our customers we only reveal company names on request and with the consent of the references.

Interested?

Call us today and ask for your individual, unbinding quotation.

- ✦ Mail: team@csnc.ch
- ✦ Phone: +41 55 214 41 60
- ✦ Internet: www.csnc.ch



Anatomy of a hacker attack

At the beginning of an attack there is basically an information gathering (footprinting) whereby the attacker looks for information on the target system in the Internet. For this purpose e.g. queries in DNS, whois databases or search engines are used and websites are interpreted.

In a second step, also called "Reconnaissance", the target network is identified and evaluated. How is the company connected to the Internet (routing)? What IP ranges are officially assigned to this company? Are systems hosted externally?

What is actually vulnerable? This question is answered in the mapping phase where with the help of a scanner active systems in the target range are determined.

As soon as the active target systems are known, a port-scanning can be started. Here the available ports for each system are detected. The aim of the subsequent Application-Mapping respectively the Application-Fingerprinting is to assign these ports/services to an application (e.g. DNS server) and if possible to identify the exact version of the software applied. As in the OS-Fingerprinting, this happens e.g. by Banner-Grabbing or through the evaluation of server specific replies.

With the knowledge about the applied software-version the attacker can in a next step search specifically for known vulnerabilities (vulnerability scanning) and, if possible, take advantage of these (Exploiting). In a Web application the search for attacking points mainly depends on the configuration and the functionality.

A final option is to search laboriously for new (unknown) vulnerabilities and/or to develop an own damage code. Alternatively specific Denial-of-Service attacks or Social Engineering may be successful.

Compass Services explained more closely

Would you like to get more information on our services? We gladly advise you in a personal discussion on these issues:

Security Reviews

Evaluation of the IT Security Policy, security architecture and implemented measures, processes and documentations or checking of the system configurations together with an administrator on site.

Vulnerability Scanning

Search for known vulnerabilities and potential configuration errors on infrastructure- (network appliances, systems) and application-level (services). These tests are executed using a scanner.

Web Application Testing

Specific examination of a Web application on weaknesses, such as Cross-Site Scripting or SQL-Injection, but also on (logical) errors in the authentication/authorisation, respectively in the session handling. These tests are to a large extent carried out manually. However, they are complemented by the use of Web-Application-Scanners.

Ethical Hacking/Penetration Testing

Here an attacker is simulated. The Compass team tries to exploit identified weaknesses systematically in order to gain unauthorised access to a computer or a network.

Social Engineering

Taking advantage of the human factor as one of the weakest links in the chain of security. For instance information may be gathered via telephone, a sent Trojan or as a service employee on site.



Example of the Compass Security Report

The security report of Compass Security mainly consists of three parts: The Management Summary, the Table of Vulnerabilities and Remediation and the Technical Report. This chapter shall give you an impression of how the Compass report looks like. Ask for our sample report to get an in-depth insight into Compass reports. We are pleased to be of your service.

Components of the report

The Management Summary gives Managers a rough overview about the main weaknesses that have been identified during the security assessment in a short non-technical security statement, enabling them to use the report as decision support.

2 Management Summary

2.1 Overall Impression

The results of the penetration test that has been conducted by Compass Security in April 2008 are considered as good. No major vulnerabilities have been identified that might circumvent proper operation of the system. Only few weaknesses with a severity of medium to low were identified and should be addressed and mitigated to assure a good security-level.

2.2 Introduction

Sample Ltd. is one of the world's leading suppliers of goods. Information technology takes a major role in the customer value chain and adequate protection against hackers and crackers is an important criterion for the future. Therefore, the customer decided to assess the company's IT infrastructure to reveal potential threats and to improve current measures.

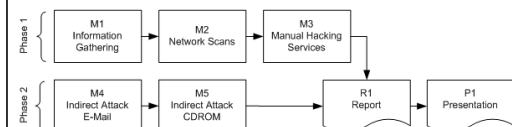
Compass Security AG is an incorporated company based in Rapperswil (SG) Switzerland that specializes in security assessments and forensic investigations. To assess the corporate IT security risk landscape of the customer Compass Security conducts a world-wide penetration test.

To speed up the whole information gathering process, some information was given to Compass Security in advance:

- + IP addresses of the target networks
- + Domain names registered by the customer
- + E-Mail addresses for the social engineering part
- + IP addresses and/or domain names of the customer core systems

2.3 Procedures

Compass Security divided the testing of the security measures into different phases and modules. The results are summarized in this report.



2.4 Results

Compass Security conducted a worldwide penetration test against the customer's corporate network. By direct attacks (phase one) and indirect attacks (phase two) Compass tried to gain access to the customer infrastructure. The conducted penetration test shows that access to systems or applications was possible by direct and indirect attacks.

2.5 Phase 1: Direct Attacks

Services with outdated patch levels having known vulnerabilities have been identified. Public exploits were not found by Compass. However, the potential risk of an existing and running exploit in the wild still remains.

Compass Security also found applications, which send login credentials over unencrypted connections. If an attacker is able to sniff the traffic he can extract the username and password from the unencrypted network traffic.

On some web applications, which offer e.g. a strong authentication with username, PIN and secure token it was possible to inject malicious code fragments. Attackers may abuse this weakness and fake the web sites content or steal a logged on user's session ticket. Having a valid session ticket allows attackers to impersonate the legitimate ticket owner. Attacking the web application with malformed parameter allowed revealing credit card numbers and application user's personal details from the database.

2.6 Phase 2: Indirect Attacks

The indirect attacks were split into different cases. U3 USB Sticks and CD-ROMs were prepared to automatically execute a Trojan, which opened an encrypted channel to a server of Compass Security. Furthermore, it was programmed to gather some specific files on the machine and transfer it to a specified server. The computers connected to the server could be controlled by Compass. Some users plugged-in the USB stick to their office computers, which then opened a channel to the Compass server.

Compass was able to take over some computers, determine their user and their location. As an evidence for the break-in, Compass downloaded some files.

2.7 Recommendations

Compass recommends implementing the following measures to improve the security level of the tested components.

- + Update and patch all Internet facing services to avoid break-ins due to outdated vulnerable service software.
- + Ensure that confidential or secret classified data such as user passwords are sent over encrypted connections only. Therefore, setup secure socket layer (SSL) communication for the affected login application.
- + The whole web application source code has to be revised for proper input validation and output encoding. Dynamic content which is sent to the client web browser has to be properly encoded using HTML entities. The dotNET framework already offers such a method `Server.HtmlEncode(String xy)`. Input



The most important and coevally part and parcel of the security report is the vulnerability table, which gives the persons in charge of the technical implementation crucial information about the weaknesses that have been identified during the security assessment. Moreover, an appraisal provides information about the severity of each weakness.

3 Vulnerabilities and Remediation

The tables in this chapter summarize the security issues found during web-application security assessment. A definition for each column is given here:

No.	Reference	Weakness	Threat	Remediation	Rating	Comments
Each issue is consecutively numbered.	Reference to the corresponding test case in the following chapters	Explains the vulnerability or weakness found during testing.	Explains what could happen if the weakness is exploited	Recommendation on how to correct the vulnerability.	Compass rating of the weakness and the corresponding threat: ●* : Low ●*●* : Medium ●*●*●* : High	Normally left blank. The customers comment regarding this issue.

3.1 Manual Hacking

No.	Reference	Weakness	Threat	Remediation	Rating	
1.	5.2.1 #1	Invalid server certificate The server makes use of an invalid sever certificate: + Invalid issuer (Self-signed certificate)	Because the certificate is not valid the browser shows always an error message. Due to these alerts, the user will not manually check the certificate each time and accepts the certificate. If the user does not check the certificate it is possible that the user is not on the right web server.	Use on the production web server a certificate which is valid and signed by a trusted CA.	●*●*	

The third part of the report is a detailed documentation of the test cases that have been conducted in the security assessment. Compass Security sets a high value on documenting all technical details in a way so that system engineers are able to understand, track and reproduce each single security issue.



5.2 Manual Hacking Services

5.2.1 Host 123.123.123.4

No.	Description of Test	Expected Result	Actual Result	PASS FAIL
Goal Manual Hacking of the detected service.				
Preparation Tools: + Hydra (www.thc.org)				
1.	Determine service.	-	HTTPS	FAIL
2.	Version?	No detailed version available.	Not available.	N/A
3.	Are there any known vulnerabilities available?	-	No. Exact version is not determinable.	N/A
4.	Valid certificate?	Yes.	No. Certificate is not signed by a trusted certificate authority.	FAIL
5.	Is it possible to guess an account?	No.	No.	PASS
6.	Check SSLv2.	Not active.	Active.	FAIL
7.	Check SSLv3	Active.	As expected.	PASS
8.	Check export and weak ciphers.	No weak ciphers in use.	Weak ciphers available. + Ciphers based on DES + Export ciphers + Ciphers based on MAC-Algorithm MD5	FAIL

```

Details Concerning No. 6
mschurte@seth:~/passlist> hydra -L c0mmon.txt -P common-passwords.txt
123.123.123.4 https-get /
WARNING: Restorefile (/hydra.restore) from a previous session found, to prevent
overwriting, you have 10 seconds to abort...
Hydra v5.2 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2006-11-24 12:43:45
[DATA] 15 tasks, 1 servers, 66086 login tries (1:01/p:016), ~4131 tries per task
[DATA] attacking service http-get on port 443
[STATUS] 406.00 tries/min, 406 tries in 00:01h, 65690 todo in 02:42h
[STATUS] 441.78 tries/min, 64942 tries in 02:27h, 1154 todo in 00:03h
[STATUS] attack finished for 123.123.123.4 [waiting for child to finish]
Hydra (http://www.thc.org) finished at 2006-11-24 15:10:42
mschurte@seth:~/passlist>

Details Concerning No. 7, 8, 9
mschurte@seth:~> ./test-ssl.sh 123.123.123.4 443
=====
Testing the Ciphers a SSL server supports
(Usage: ./test-ssl.sh host port)
=====
Supported ciphers with SSLv2 by 123.123.123.4
=====
EXP-RC4-MD5
RC4-MD5
=====
Supported ciphers with SSLv3 by 123.123.123.4
=====
DES-CBC3-SHA
DES-CBC-SHA
EXP-DES-CBC-SHA
EXP-RC2-CBC-MD5
EXP-RC4-MD5
IDEA-CBC-SHA
NULL-MD5
NULL-SHA
RC4-MD5
RC4-SHA
=====
Supported ciphers with TLSv1 by 123.123.123.4
=====
DES-CBC3-SHA
DES-CBC-SHA
EXP-DES-CBC-SHA
EXP-RC2-CBC-MD5
EXP-RC4-MD5
IDEA-CBC-SHA
NULL-MD5
NULL-SHA
RC4-MD5
RC4-SHA
  
```