

IT SECURITY TESTING

Security Assessments

The security assessments are checked using the OSSTMM v3 methodology.

Internet security assessment answers the question "How easy is it to hack into the company from the Internet?" The scope of this test includes every equipment accessible from the Internet, such as web, mail, FTP and VPN servers, routers, and firewalls. The result of the test is a list of security vulnerabilities discovered in the Internet-facing systems with recommendations to remediate them.

The starting point can be: the name of the company only, or an Internet domain name, or a list of specific IP addresses provided by the customer, etc...

The information gathering phase will allow us to "better know our enemy": people names, phone number ranges, email addresses, Internet domains, IP ranges, IT technologies used, etc...

The contact phase will identify hosts accessible or not as well as the network path to reach them. The list of hosts discovered as well as the guessed network architecture is given to the customer for approval.

Having an approved list of systems to investigate, the attack phase is performed. It consists of automated vulnerability scan and manual tests targeting each system. Then we will

try to exploit the vulnerabilities in order to eliminate false-positives. If exploiting the vulnerability might have an impact on the host, the customer is contacted first in order to have its agreement to proceed further.

Internet security assessment usually excludes custom web applications which are covered by the web application test offer.



An **internal network security assessment** simulates an attack done by a malicious insider. The test can be performed with no initial access except a network connection or with normal user-level privileges. The test can also include a "stolen laptop" (or a standard desktop) scenario to check what information an attacker can retrieve from it. The test may also include "physical access" check to see if a user can gain Administrator privileges on its own or someone else's workstation by abusing physical access to it.

An internal network security assessment starts with network mapping whose goal is to identify servers, workstations & laptops, printers, routers, switches and other devices connected to the network as well as the function of each server (domain controllers, database servers, application servers, file servers, etc...).

The attack phase consists of checking for security problems: security patches applied? Systems securely configured? Can Passwords be obtained & cracked? ...

As a result the customer gets a complete view of the internal network security. The report includes the list of discovered vulnerabilities, the risks they induce and their impact. For example: "The Windows servers are not regularly patched, meaning that anybody connected to the corporate network can use one of the publicly available exploits in order to gain complete control over domain controllers, and thus have complete ownership of the network." The report also includes recommendations for mitigating the problems.

Definitions

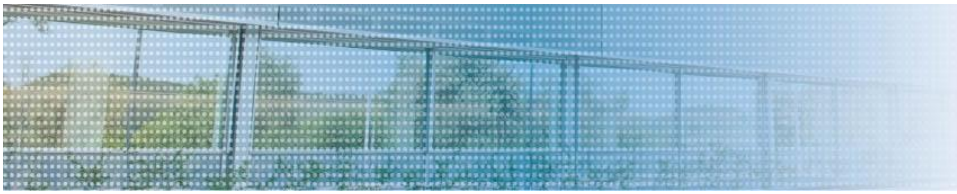
A **penetration test** simulates a hacker attacking the company with the goal of penetrating as deep as possible into the company network and gain access to confidential data. Such a test is recommended when there is a need to demonstrate to the top management that IT security requires more attention, support and budget.

A **security assessment** is designed to provide a detailed view of the level of security of the customer's network. The goal is to find a maximum number of security weaknesses in the systems connected to the network. Each identified vulnerability may be manually verified and its impact assessed in the context of the customer's setup. Security assessments can be performed from Internet (to measure the exposure to external intruders) or from internal network (to assess the exposure to malicious insiders). A security assessment can have a scope as wide as the whole customer's network or focused on a restricted number of systems set up for a particular project.

Web applications can be tested from an outsider or authorized user perspective. We also offer source code reviews, which is the most effective way of finding security bugs in applications.

Specialized tests include Wi-Fi, PBX and dial-up, VoIP, RAS and VPN tests.

A **configuration review** provides an in-depth analysis of systems' security. Recommended on newly implemented systems.



Web application security testing

A buggy web application can lead to a complete infrastructure compromise. Web applications can suffer from all kinds of problems going from remote code injection (an attacker can force the application to execute arbitrary code), to access control problems (one user can view another users' private data).

ebrc Consulting Services offers in-depth security analysis of web applications, including if needed a **source code review**. We have extensive experience testing various web applications.

Web applications are checked using the **OWASP v3** methodology which has 66 controls points covering the following problems:

Information gathering. What information is disclosed?

Configuration management. Are there SSL weaknesses? Is the DB

listener accessible? Are there old, backup or unreferenced files accessible?

Authentication. Does the application provide strong enough authentication? Are there any ways to bypass authentication? Are password management mechanisms (password reset & change) securely implemented?

Session management. How is session management implemented? Is it possible to predict or guess session tokens/cookies?

Authorization. Are authorization checks consistently implemented? Is it possible to access pages of the application without authorization? Is it possible to perform actions that should require authorization without any authorization? Is privilege escalation possible?

Business logic. Is it possible to make the application do something unexpected, for example, buy negative amount of items, or bypass order payment?

Data validation. Does the application properly handle user input? Cross-Site Scripting? Is it possible to do injections (SQL Injection, LDAP Injection, XML injection, SSI injection, Xpath injection, Code injection...)?

Denial of Service. Is it possible to lockout users? Are there some buffer overflows that can crash the application?

Web services. Are there some WSDL weaknesses? SOAP testing. Replay testing.

Ajax testing. Are there any AJAX weakness?

Specialized tests

ebrc Consulting Services offers several specialized tests for advanced technology areas. These can be part of a full-scale penetration test, or they can be performed independently.

Wireless tests (Wi-Fi, Bluetooth). Insecurely configured wireless networks often provide an entry point into an organization's network. Securing wireless networks is further complicated by the fact that earlier security technologies such as WEP are now known to be badly flawed.

Our **dedicated wireless network assessment** tests the security of authorized wireless networks. It will also allow the discovery of rogue access points (e.g. users who have connected such an access point on their own to your internal network).

PABX tests and War-Dials. Now that broadband Internet connectivity is nearly ubiquitous, the security of phone lines, which may provide an alternative access method into your organization, is often overlooked.

In this context, **ebrc Consulting Services** offers a security audit of PABX facilities. We find that for this kind of installation, broad access can often be obtained from outside the company by using undocumented features or by guessing the appropriate PIN codes. This may allow attackers to access your voice mail, or to make international calls using your infrastructure.

ebrc Consulting Services can also perform so-called war dials. This kind of test looks for insecure dial-in access to your organization. Typical examples of this include illicit modems installed by users, and vendor maintenance dial-in facilities.

VoIP. The convergence of voice and data traffic offers interesting cost-saving and flexibility opportunities. However, at the same time this integration increases the risks to your organization (e.g. by rendering voice traffic vulnerable to disclosure via sniffing attacks).

A VoIP audit will allow assessing your exposure. Topics covered in-

clude the VoIP topology and authentication framework. Also, it will check specific infrastructure-related security issues (e.g. vulnerabilities for particular devices).



Remote access tests.

Today a lot of companies offer their employees remote access to the corporate network. Such systems increase productivity but also provide additional entry points for hacking attacks.

We have experience in security testing of various remote access solutions, such as dial-in servers, IPsec and SSL VPNs and GPRS. The tests can be performed from a perspective of a malicious outsider who attempts to connect to the corporate network. In a "stolen device scenario" we test if an attacker who has stolen a company laptop or a PDA can use it to gain access to the corporate network. The test can also include a configuration review of server- and client-side devices.