



Assess your vulnerability!



OSSTM

Hacking
test

PCI DSS

2700X

- Penetration tests
- Verification audits
- Configuration audits
- Applications code audits
- Real time Security audits by **IKARE**

A comprehensive **intruding audit** is composed of three phases:

- a « **black box** » audit, also qualified of blind test, since the investigated technical architecture is unknown (the hacker script),
- a « **white box** » audit the architecture is provided allowing a better targeting of the test (script of the ex-trainee)
- an audit on user account, aiming to measure the internal nuisance capacity (script of a malicious employee).

In order to master the impacts of the tests, a **legal contract** engaging the different concerned parties is signed and a plan of tests underlining their stakes and their impacts (in term of confidentiality, integrity and availability), is submitted to validation before each phase.

Why call on ITrust for an audit?

In order to get a comprehensive, independent and uncommitted vision of your security and to get concrete recommendations, immediately applicable.

A Security audit on what targets?

- audit of infrastructures of access to the Internet, of extranets, of distant accesses
- audit of telecom infrastructures
- flux and network data audit
- on-board systems audit
- PABX audit
- wireless network audit
- process and organization audit
- Applicative architectures audit, applications audit and code audit
- Investigation audit.

What type of audit?

Verification audit

Analysis of the state of a system or of a network, regarding to the organization, the architecture, the configurations, the exploitation and skills. It is both a comprehensive and technical approach, based on the methodology and the experience of ITrust; the audit is performed with the operators, in a delimited area.

Certification audit

Assessment addressing the state of the system compared to a reference, for example the respect of defined security requirements (27001, PCI/DSS, FIPS, ...).