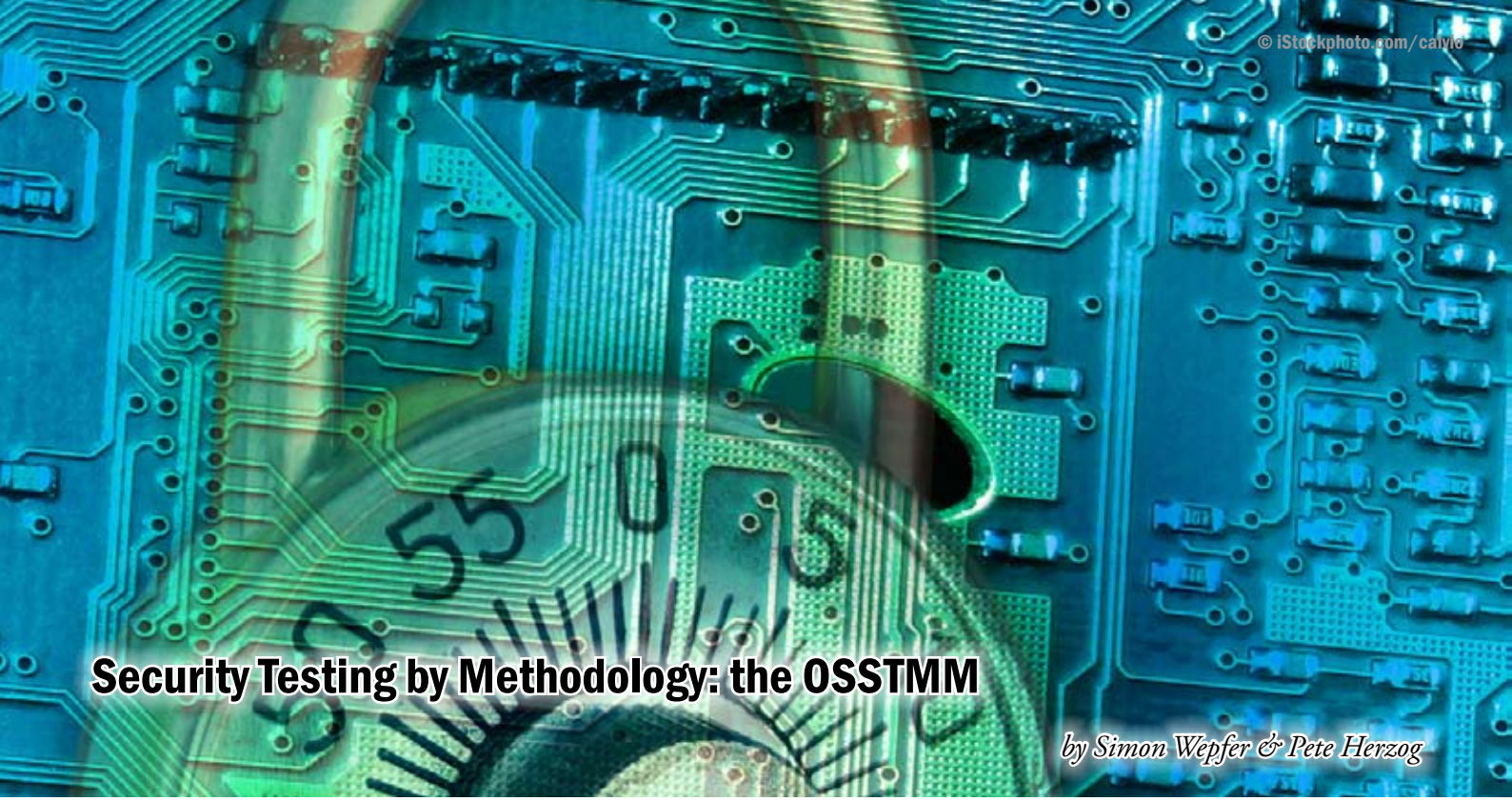
June, 2009

testing experience

The Magazine for Professional Testers

printed in Germany
print version 8,00 €
free digital version
www.testingexperience.com
ISSN 1866-5705

Security Testing



Security Testing by Methodology: the OSSTMM

by Simon Wepfer & Pete Herzog

Security tests are an important part of the risk management process and executives realize the benefits of an independent security test: It introduces a neutral view on the target and can improve security when the proposed sensible measures are successfully applied. But there are often also questions to answer after such an audit.

How secure is the target, and are there aspects that have not been tested? How much has our security improved since the last test? How does our security compare to other companies in our industry? This article is a brief introduction into the Open Source Security Testing Methodology Manual (OSSTMM), which can answer these and other follow-up questions.

OSSTMM is a freely available manual that provides a methodology for a thorough security test of physical, human (processes) and communication systems. A core aspect are the security metrics – the Risk Assessment Values (RAV) – which express the final security level of the tested system as a numerical value. The current release candidate of OSSTMM 3.0 is an approximately 150-page document and is a complete re-write from the 2.X version series incorporating the results of the last 6 years of research.

The main purpose of the OSSTMM is to provide a scientific methodology for the accurate characterization of operational security and is adaptable for penetration tests, ethical hacking, security assessments and so forth. In the EU-sponsored project, Open TC, it became the standard for testing and measuring trusted computing systems. Most of all, an OSSTMM compliant test defines the target clearly, and results are reproducible, something unusual in the current methods of ethical hacking and penetration testing.

Preparation and Testing

Before the test can actually start, the assets that have to be secured must be defined. The protection mechanism for the assets are the targets to test. The engagement zone is the area around the assets, the test scope is everything needed to keep the assets operational, for instance, processes or network protocols. The test vector defines the interaction points of the scope. For instance, a DMZ may be tested from the internet or from the LAN as well – with obviously different results. Then, the testing channels have to be defined. Our example DMZ may be tested not only on the communication layer but on the process layer as well (e.g. patching process).

The test type defines the knowledge about the target and the test. Common known testing types are black box and white box; the OSSTMM, however, distinguishes six types, each detailing different results. The rules of engagement are protecting the customer and the tester on legal, ethical and procedural aspects.

When all the above has been defined well, it is clear which tests in the OSSTMM have to be performed on the scope. OSSTMM tests define only what is to be done, but do not dictate any tools. One test for data networks for example is requesting that server uptime has to be verified to latest vulnerabilities and patch releases. Another example is that responses to UDP packets with bad checksums to a collection of ports have to be verified. The tools to use and how to use them is left up to the tester.

Classification	Description
Vulnerability	is the flaw or error that: (a) denies access to assets for authorized people or processes, (b) allows for privileged access to assets to unauthorized people or processes, or (c) allows unauthorized people or processes to hide assets or themselves within the scope
Weakness	is the flaw or error that disrupts, reduces, abuses, or nullifies specifically the effects of the five interactivity controls: authentication, indemnification, resistance, subjugation, and continuity.
Concern	is the flaw or error that disrupts, reduces, abuses, or nullifies the effects of the flow or execution of the five process controls: non-repudiation, confidentiality, privacy, integrity, and alarm.
Exposure	is an unjustifiable action, flaw, or error that provides direct or indirect visibility of targets or assets within the chosen scope channel.
Anomaly	is any unidentifiable or unknown element which has not been controlled and cannot be accounted for in normal operations.

An OSSTMM compliant test is much more than running an automated vulnerability scanner and printing the report. It relies on the tester's in-depth knowledge and experience, and on human intelligence for interpreting the results. This does not mean that automated tools will not be used at all, but they will be used as what they are: just a tool without real intelligence.

Risk Assessment Value

Once a risk is detected and verified, it has to be categorized. OSSTMM is naming these limitations; the inability of protection mechanisms to work correctly, see table

OSSTMM knows five „risk" classifications

The limitations are one of the three factors for calculating the final RAV. The operational security is a second one, derived from visibility (a means of calculating opportunity for an attack), access (counting the interactive access points) and trust (fall-back to unauthenticated access to trusted systems). The third factor for calculating the RAV are the controls implemented for each point identified in the operational security section. Controls are grouped in class A (authentication, indemnification, subjugation, continuity and resilience) and class B (non-repudiation, confidentiality, privacy, integrity and alarm).

Certification

ISECOM (Institute for Security and Open Methodologies) offers several OSSTMM-specific certification and training schemes. The ISECOM Licensed Auditor (ILA) program provides quality assurance and support for obtaining OSSTMM certified audits from a properly accredited auditing company. OPST (OSSTMM Professional Security Tester) and OPSA (... Analyst) is a certification for persons. Additional information may be found on http://www.isecom.org/.

Biography

Simon Wepfer is COO at OneConsult.

Pete Herzog is founder of the OSSTMM and Director of ISECOM.