IT Security Management

Penetration Tests

IT systems with connections to public or private networks, thus internally and externally accessible, are exposed to unauthorised, mainly anonymous access attempts. To address this security issue, a methodology is required that creates realistic testing conditions from an attacker's point of view. A penetration test fulfills these requirements: it is a controlled attempt to penetrate an IT system based on the same tools and techniques an attacker would use. This approach helps you gain valuable information about technical, but also organisational and conceptual weaknesses of your company's IT infrastructure.

Types

Penetration tests can be designed individually to meet various different test objectives. For example, the amount of information the tester is provided with or the level of aggressiveness he uses can be adapted to your specific requirements to ensure effective and efficient completion at a calculated risk. As a standardised basis for our penetration tests, we use the "Open Source Security Testing Methodology Manual" (OSSTMM), the "Open Source Web Application Security Project" (OWASP), as well as the concepts developed by the German Federal Office for Information Security (BSI).

For more detailed information about the methods mentioned, please refer to the following websites:

- http://www.isecom.org/osstmm/
- http://www.owasp.org/
- http://www.bsi.de/EN

Procedure

The penetration test consists of 5 phases:

1. **Preparation** – At the beginning of the project, we work with you to define the objectives, scope, types, processes, and objects of the penetration test. Furthermore, we discuss with you the potential risks that the selected penetration test implies as well as appropriate emergency measures.
2. **Collecting Information** – This phase serves for our penetration testers to gain a comprehensive and detailed overview of the installed systems including their potential vulnerabilities. Test modules are, among other things, the evaluation of publicly available data such as DNS or WHOIS, various port and application scans, OS fingerprinting, collection of FTP and web server file structures, web cookie examination, web server session handling, and investigation of vulnerabilities. A white-box test additionally includes various other checks, e.g. of the security-relevant operating system, application configuration files, or patch levels.
3. **Evaluation/Risk Analysis** – The information collected in phase 2 is now evaluated and analysed. This serves as the basis for the selection of targets to attack in phase 4.
4. **Active Intrusion Attempts** – Based on the results from the previous phases, we actively attack the selected systems applying the following modules: password cracking, buffer overflow exploits, cross-site scripting, SQL injection, session hijacking, and social engineering.
5. **Final Analysis** – Upon test completion, we provide you with a comprehensive report that summarises all findings. It includes a risk rating for each vulnerability as well as recommended security controls to address these weaknesses.

Result

The recommendations in the final report are a guideline for you to effectively and efficently eliminate the identified IT infrastructure weaknesses. This gives you the opportunity to substantially improve the IT security level in your organisation.

plan42

plan42 is a consulting firm specialised on IT Service Management, IT Security Management & Business Solutions. Process analysis, consulting, conception, and implementation – plan42 combines technical expertise and best-practice concepts of IT Service & Security Management.