



Highly qualified customer adjusted security audits and penetration tests are our key services. We have created us a very good name in the sector of IT-Security and our employees are seen as the leading security experts in europe and in the world. We use cutting edge self written state of the art tools and knowledge when conducting security audits. See this partial list of major grade vulnerabilities we discovered in the past:

- Microsoft Internet Information Services FTPd Remote Vulnerabilities
- Apache Remote Denial of Service in the svn module
- Microsoft IIS WebDAV Remote Authentication Bypass
- FreeBSD 7.0-Release Remote Exploit in the telnet daemon
- Oracle Weblogic Remote Arbitrary Code Execution
- SunOS 5.10/5.11 in.telnetd Remote Authentication Bypass

KC Security is also able to discover vulnerabilities in any software at a customer request. This means we get paid for finding zero-days or write Private Exploits for known bugs and advisories.

Contact KC Security electronically at nikolaos@rangos.de



Core Services: Security Audits

- 1** Penetration Tests (Infrastructure Tests, Web Application Tests)
- 2** Source code analysis
- 3** Binary Analysis
- 4** System Hardening

1 Penetration Tests and System Hardening

The service named Penetration Test is the analysis of objects and systems in a corporate architecture. The service named System Hardening includes hardening Windows and UNIX based operating systems.

Customer projects are conducted in the NSA IAM way:

- Pre-Assessment
 - Determine and manage the customer's expectations
 - Gain an understanding of the organization's information criticality
 - Determine customer's goals and objectives
 - Determine the system boundaries
 - Coordinate with customer
 - Request documentation
- On-Site Assessment
 - Conduct opening meeting
 - Gather and validate system information (via interview, system demonstration, and document review)
 - Analyze assessment information
 - Develop initial recommendations

- Present out-brief

- Post-Assessment
 - Additional review of documentation
 - Additional expertise (get help understanding what you learned)
 - Report coordination (and writing)

2 Source code analysis in nearly all programming languages

During a Penetration Test it is possible that the source code of the running software is checked for vulnerabilities. Dedicated source code audits on existing source codes are also possible.

3 Binary analysis

The service binary analysis is for example auditing and assessing the risk of Malware (Virii and Trojans)

4 System Hardening

The service named System Hardening includes hardening Windows and UNIX based operating systems.



Profile and knowledge

As consultants we are in possession of the following special knowledge:

- Methods to intrude into systems and networks
- Analysis of critical infrastructure
- Vulnerability and risk analysis
- UNIX / Linux operating systems and environments
- Microsoft Windows operating systems and applications
- Binary analysis
- Software source code auditing
- Secure network design
- Database security
- Forensics