SQuirreL Suite

In an age of ever escalating threats ensuring that sensitive data remains confidential is a significant concern to many organisations. Whether it's financial accounts, client information, sales records or human resource details, keeping both your information and that of your clients secure is of paramount importance.

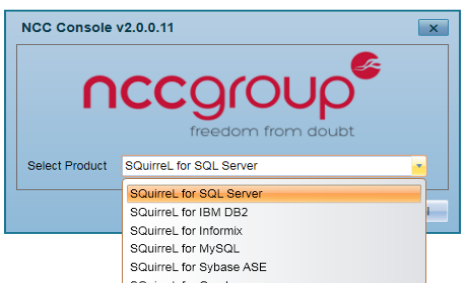
Adequately ensuring that database security is maintained is a challenge that must be met and overcome in order to minimise security threats.

SQuirreL Suite provides you with a helping hand from the database security experts.

NCC Group's extensive experience and expertise within the IT security services industry allows us to develop and deliver the most powerful vulnerability assessment scanner available for database servers.

NCC Group's SQuirreL Suite provides peace of mind by detecting and fixing security issues while maintaining the security of your databases.

SQuirreL Suite supports RDMS for Microsoft SQL Server, Oracle, MySQL, IBM's DB2, IBM's Informix and Sybase ASE as well as the popular systems MongoDB and PostgreSQL.



The console allows users to select the relevant version of SQuirreL Suite in order to perform a focused audit.

Product overview

SQuirreL for Microsoft SQL Server: An innovative vulnerability assessment tool specifically developed to scan Microsoft SQL Server 7, 2000, 2005, 2008, 2012 and 2014 infrastructures.

Unlike many of the conventional applications available SQuirreL for SQL Server allows users to generate bespoke solutions that can be applied to servers, ensuring the security of databases are maintained.

SQuirreL for Oracle: The best defence against threats to your database security. Whether used in the enterprise or for single server networks. SQuirreL provides an easy mechanism for quickly securing the Oracle infrastructure. As well as finding all of the security holes, SQuirreL for Oracle can fix them too.

SQuirreL for Oracle is compatible with Cyber Ark Enterprise Password Vault (EPV), part of the Cyber Ark Privileged Identity Management (PIM) System. Supports Oracle 8 through 12c.

SQuirreL for MySQL: Has been specifically developed to scan MySQL 4.1, 5.0, 5.1, 5.5, 5.6 and 5.7 infrastructures. Details of all vulnerabilities can then be viewed in full covering, description, solution, references and compliance.

SQuirreL for DB2: Supports scanning of IBM's leading database server product. You can manage a multitude of vulnerabilities or bad practices on your database servers - right down to individual tables. SQuirreL for DB2 supports scanning of v7x, 8x, 9x and 10x.

SQuirreL for Informix: Assesses the risk posed by security threats of IBM's Informix relational database management system, helping to understand and minimise any potential threats that may exist. In an enterprise environment that demands factors of performance, scalability and reliability security issues with IBM's Informix can represent a serious threat to business continuity.

SQuirreL for Sybase ASE: Provides an effective and comprehensive automated scanning tool able to quickly assess the security posture of your Sybase database environments. SQuirreL for Sybase supports scanning of Sybase ASE all versions up to and including 15.7.

SQuirreL for MongoDB: Allows database administrators and security professionals to identify vulnerabilities such as missing patches, weak passwords, excessive permissions and a lack of encryption. Comparative scanning then provides confirmation that fixes to these issues have been applied.

SQuirreL for PostgreSQL: Provides security checks for one of the fastest growing systems on the market.

Features & benefits

Variable audits

The software permits users to conduct variable levels of audit. The user has full control over all the checks that are performed and, via the graphical user interface, can change these ahead of any scans. The selections that are checked against can be changed to your needs with various choices that can be made to provide total flexibility.

The unique ability to adjust the depth at which the SQuirreL Suite conducts its audits allows system administrators to mold the application to their requirements.

Comprehensive

SQuirreL Suite scours servers for thousands of potential security vulnerabilities. The application routinely checks for patch levels, objects and statement permissions, login and password authentication mechanisms, stored procedures, start-up procedures, including checks for unencrypted sensitive data such as credit card or social security numbers.

Compliance

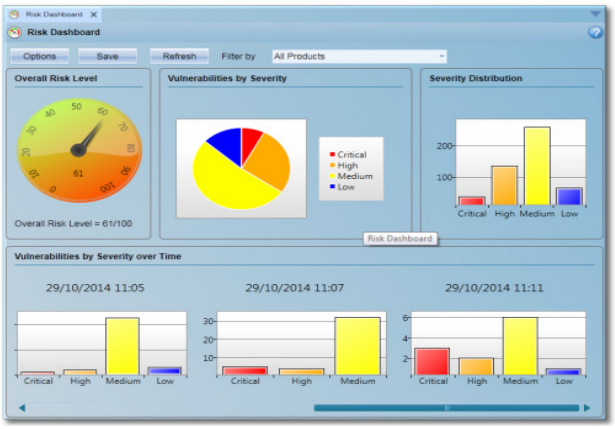
With the need to comply with the latest industry standards SQuirreL Suite supports a range of compliance templates. The software supports compliance checking for: Payment Card Industry (PCI), Sarbanes –Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach Bliley Act (GLBA), National Institute of Standards and Technology (NIST SP 800-53), Defense Information Systems Agency (DISA), Center for Internet Security Benchmarks (CIS), Framework for Improving Critical Infrastructure Cybersecurity (FICIC) and International Organisation for Standardisation (ISO 27001).

Reporting

SQuirreL Suite provides a range of output formats for scan results including Text, RTF, HTML, PDF, XML and CSV. Comparative reporting enables the user to compare two identical scans over time and uncover new, fixed and persisting vulnerabilities. This functionality allows trend analysis to be performed over time.

A new report designed system produces a highly flexible set of reporting options. This feature provides complete freedom to create bespoke reports with a comprehensive range of data filtering capabilities.

The risk dashboard is a high level overview for all the scan result data. This informational screen provides diagrams to represent the overall level of security and the total number of vulnerabilities discovered. A typical example of this is shown below



CVE compatibility

Common Vulnerabilities and Exposures (CVE®) is a dictionary of common names (CVE Identifiers) for publicly known information on security vulnerabilities and is now the industry standard for vulnerability and exposure naming. CVE Identifiers provide reference points for data exchange so that information security products and services can co-ordinate with each other. SQuirreL Suite supports CVE.

Security browser

The SQuirreL Security Browser (SQL and Oracle) is an integrated component that allows the user to browse and audit the security settings of the database or instance. The security browser also allows the user to create custom checks to monitor users and permissions within the database.

One click fix

A feature of SQuirreL Suite is the ability to generate SQL Lockdown Scripts. When SQuirreL Suite discovers vulnerabilities it can generate lockdown scripts that can be employed to remedy any issues.

Always up-to-date

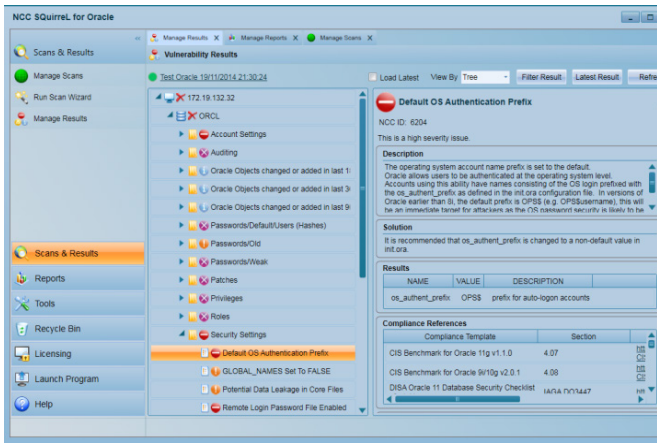
Because the security landscape is in a continual state of flux, it is vital that administrators gain access to the latest known vulnerabilities. SQuirreL Suite is supplied with an ongoing support contract that allows users to download updated vulnerability definitions for the application database on a regular basis.

As well as assessing the security of database servers based upon known vulnerabilities, it also routinely scans for as yet unpublished vulnerabilities that have been discovered by NCC Group's security research team.

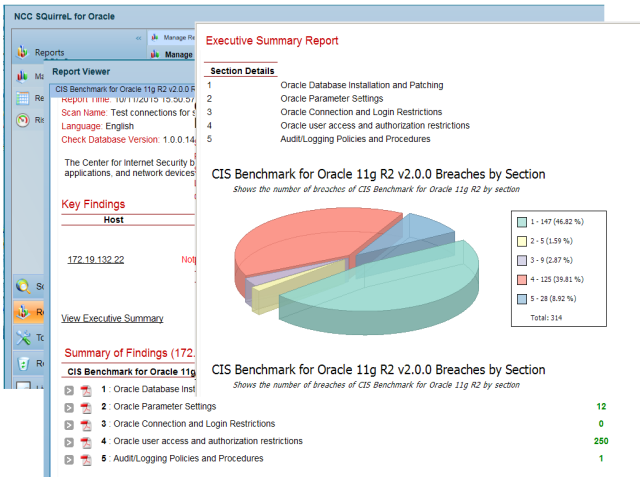
Other features & benefits

- Checks for elevated system access in start-up procedures or stored procedures.
- The testing notes feature allows the user to add custom assessment notes for the selected host or instance. The information entered here can be added to the final report.
- Detects and reports on a multitude of issues including buffer overflows, weak passwords, PL/SQL Injection, dangerous privileges, weak default settings, weak and dangerous object privileges, backdoors, XML database security and Oracle internet directory issues. Allows DBAs to fix security holes and perform password audits.
- Non-intrusive and safe to use, the software will not alter the database in any way.
- Dictionary password audits are performed as standard during vulnerability scans.

Manage results



Executive summary report



System requirements

- Microsoft Windows 7 SP1/Windows Server 2008 R2 or later.
- 15GB free disk space.

About NCC Group

NCC Group is a global expert in cyber security and risk mitigation, working with businesses to protect their brand, value andreputation against the ever-evolving threat landscape.

With our knowledge, experience andglobal footprint, we are best placed to help businesses identify, assess, mitigate and respond to the risks they face.

We are passionate about making the Internet safer and revolutionising the way in which organisations think about cyber security.

+44 (0) 161 209 5200 response@nccgroup.trust www.nccgroup.trust

NCCGISSSQLSV20517