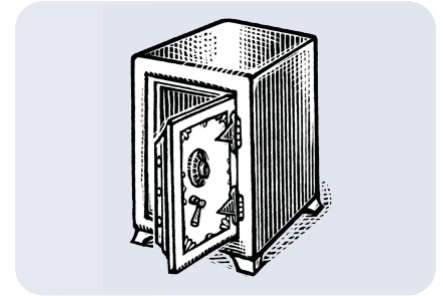


NGSSQLCrack



Microsoft SQL Server is a relational database management system that forms an integral part of the BackOffice family of servers. In a business environment that demands factors of performance, scalability and reliability, SQL Server provides. With sophisticated back office systems come a range of vulnerabilities and risk factors, which can lead to a decrease in productivity, lost revenues, and stolen data.

NGSSQLCrack is an innovative password-cracking utility for Microsoft SQL Server that can assist enterprises in securing their infrastructures. NGSSQLCrack allows system administrators to quickly scan systems for weak passwords that are susceptible to brute force attacks, and guard against them.

Weak passwords are acknowledged as being a significant threat to enterprise level security, however they are easy to guard against. Password auditing is a proven technique for minimising risk exposure, and identifying user accounts with weak passwords.

» Product Overview

NGSSQLCrack forms part of NGSSoftware's suite of Intelligent Next Generation Security Assessment tools. The application has been specifically developed to enable administrators to quickly and easily discover insecure SQL Server passwords, and can be deployed in a variety of audit situations.

SQL Server does not store passwords internally; it stores hashes of passwords. These hashes are the result of applying a one-way function (SHA, the Secure Hashing Algorithm) to the text of the password combined with a 'salt', or 'random' value. The hash of the upper-case version of the password is stored along with the hash of the mixed-case version, and the salt is stored along with these 2 hashes. All of this can be easily guessed by observing the hash values for different passwords.

NGSSQLCrack conducts a variety of attacks against SQL Server password hashes to discover insecure passwords.

There are two aspects to the auditing process within NGSSQLCrack. These are:

- » Dictionary attack - using a 200,000-word dictionary (with the capability of adding custom dictionaries).
- » Brute Force attack - using various character combinations (including support for prefixes and suffixes).

» Features and Benefits

NGSSQLCrack has a number of key benefits, these include:

» Flexible Reporting

Because performing a thorough password audit can sometimes be a demanding process, NGSSQLCrack allows users to temporarily terminate an audit at any stage. A password crack file can be saved at any point during the audit process, and then restarted on a more convenient occasion.

» Speed

NGSSQLCrack is one of the fastest password auditing tools currently available for SQL Servers. On a 1GHz Pentium with 256 MB RAM, NGSSQLCrack can perform a 200,000-word dictionary sweep in two seconds (on a single password hash) and over 500,000 attempts a second whilst in brute force mode.

» Ease of Use and Accessibility

NGSSQLCrack is an intuitive and easily deployed application. Detailed documentation and the point and click functionality of the product allows even inexperienced administrators to quickly enumerate weak passwords. For more advanced users, NGSSQLCrack also has a wide range of customisable options.

» Other Features and Benefits

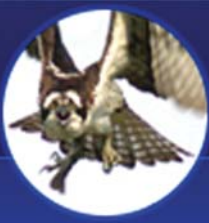
Familiar GUI based tool.

Only 'sa' login and local admin can access password hashes.

Password hashes can be retrieved directly from the SQL server.

Password hashes can be pasted from Query Analyzer.

Cost effective, requiring minimal time and labour to use.



NGSSQLCrack

» System Requirements

System: Microsoft Windows NT 4.0 (Service pack 6a)
Microsoft Windows Server 2003
Microsoft Windows 2000
Microsoft Windows XP
Hardware: 500MHz Pentium III (minimum)
Memory: 512Mb RAM (minimum)
Diskspace: 20Mb free disk space
Other Software Requirements: Microsoft SQL Server 7 & 2000

Username	Hash	Upper Case Password	Mixed Case Password
baduser	0x0100F61B7724FCAA81C...	BADUSER	baduser
BUILTIN\Administrators	NULL (blank or not an...	NULL	NULL
foo	0x010065177E6DBF8C30E...	FOO	foo
newuser	0x0100AD5D2D206F6A203...	NEWUSER	newuser
ngs	0x01005A6B869E310710...		
test			

Crack Status: Running

SQLCrack
Copyright 2002-2003 Next Generation Security Software

This computer program is protected by international laws and copyright treaties