

[TOOL] Oracle Auditing Tools

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0104.html>

From: support@securiteam.com

Date: 01/22/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 22 Jan 2002 16:10:07 +0100 (CET)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Oracle Auditing Tools

DETAILS

The Oracle Auditing Tools are designed to check Oracle servers on the Microsoft Windows platform.

The OAT use CREATE LIBRARY to access the WinExec function in the kernel32.dll. Having access to this function makes it possible to execute anything on the server with same permissions as the user who has started the Oracle Service. This means that all accounts with default passwords, or easy guessable password having this privilege can do this.

The OAT has a built-in TFTP server for making file transfers easy. The TFTPd server is based on the server source from <http://www.gordian.com>

The Tools are Java based and were tested on both Windows and Linux. They should hopefully also run on any other Java platform.

The toolkit consists of the following tools:

OracleSamDump -- Connects to the Oracle server and executes TFTP get, to fetch the pwdump2 binary. The server is then pwdump2ed and the result is returned to the SAM folder of the TFTP server.

Securiteam: [TOOL] Oracle Auditing Tools

OracleSysExec – Can be run in interactive mode, letting the user specify commands to be executed by the server or in automatic mode. In automatic mode, netcat is TFTPd over to the server and binds a shell to the tcp port 31337.

OracleTNSCtrl – is used to query the TNS listener for various information, like the Oracle lsnrctl utility. It is somewhat limited though. Use the help command to see commands currently implemented.

Requirements:

Java Runtime Environment <<http://www.javasoft.com>>
<http://www.javasoft.com>

Oracle JDBC Driver (classes111.zip or classes12.zip)
<<http://www.oracle.com>> <http://www.oracle.com>

ADDITIONAL INFORMATION

The tool can be downloaded from:

<<http://www.cqure.net/tools07.html>> <http://www.cqure.net/tools07.html>

The information has been provided by <<mailto:patrik@cqure.net>> Patrik Karlsson.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[NT] CyberStop Web Server Remote DoS"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)