

NETWORK ANALYSIS

Connect

User Name Password Log in

Remember Me?

Help Register

Home Forum What's New?

FAQ Calendar Forum Actions Quick Links

Advanced Search

Forum Resource Network Tools RATS - Rough Auditing Tool for Security

FREE

Network Monitor, Analyze & Troubleshoot

A must-have all-in-one freeware for network administrators

Learn More

If this is your first visit, be sure to check out the [FAQ](#) by clicking the link above. You may have to [register](#) before you can post: click the register link above to proceed. To start viewing messages, select the forum that you want to visit from the selection below.

+ Reply to Thread

Results 1 to 1 of 1

Thread: [RATS - Rough Auditing Tool for Security](#)

Like

Sign Up

 to see what your friends like.


Thread Tools Display

10-14-2010 05:45 AM #1

Raytan

Administrator

NewbieNetywork Analysis Master



Join Date: Aug 2010

Posts: 615

RATS - Rough Auditing Tool for Security

1 of 3

7/04/14 10:24 AM

RATS - Rough Auditing Tool for Security - is an open source tool developed and maintained by Secure Software security engineers. [Secure Software was acquired by Fortify Software, Inc.](#) RATS is a tool for scanning C, C++, Perl, PHP and Python source code and flagging common security related programming errors such as buffer overflows and TOCTOU (Time Of Check, Time Of Use) race conditions.

RATS scanning tool provides a security analyst with a list of potential trouble spots on which to focus, along with describing the problem, and potentially suggest remedies. It also provides a relative assessment of the potential severity of each problem, to better help an auditor prioritize. This tool also performs some basic analysis to try to rule out conditions that are obviously not problems.

As its name implies, the tool performs only a rough analysis of source code. It will not find every error and will also find things that are not errors. Manual inspection of your code is still necessary, but greatly aided with this tool.

Download RATS

RATS is free software. You may copy, distribute, and modify it under the terms of the GNU Public License.

Latest Release: 2.3

- Source tarball: [rats-2.3.tar.gz](#) [382K] [MD5]
- Win32 binary: [\\*\\*rats-2.3-win32.zip](#) [220K] [MD5]

Requirements

RATS requires expat to be installed in order to build and run. Expat is often installed in `/usr/local/lib` and `/usr/local/include`. On some systems, you will need to specify `--with-expat-lib` and `--with-expat-include` options to configure so that it can find your installation of the library and header.

Expat can be found at: <http://expat.sourceforge.net/>

Installation

Building and installation of RATS is simple. To build, you simply need to run the configuration shell script in the distribution's top-level directory:

`./configure`

The configuration script is a standard autoconf generation configuration script and accepts many options. Run configure with the `--help` option to see what options are available.

Once the configuration script has completed successfully, simply run make in the distribution's top-level directory to build the program:

`*`

`make`

`*`

By default, RATS will be installed to `/usr/local/bin` and its vulnerability database will be installed to `/usr/local/lib`. You may change the installation directories of both with the `--prefix` option to configure. You may optionally use the `--bindir` and `--datadir` to specify more precise locations for the files that are installed.

To install after building, simply run make with the install target:

`*`

`make install`

`*`

This will copy the built binary, rats, to the binary installation directory and the vulnerability database, rats.xml, to the data installation directory.

Running RATS

Once you have built and installed RATS, it's time to start auditing your software! RATS accepts a few command line options that will be described here and accepts a list of files to audit on the command line. If no files to audit are specified, stdin will be used.

Usage:

`*`

`rats [-d ] [-h] [-r] [-w ] [-x] [file1 file2 ... fileN]`

`*`

Options explained:

- **-d** Specifies a vulnerability database to be loaded. You may have multiple `-d` options and each database specified will be loaded.
- **-h** Displays a brief usage summary
- **-i** Causes a list of function calls that were used which accept external input to be produced at the end of the vulnerability report.
- **-l** Force the specified language to be used regardless of filename extension. Currently valid language names are "c", "perl", "php" and "python".
- **-r** Causes references to vulnerable function calls that are not being used as calls themselves to be reported.
- **-w** Sets the warning level. Valid levels are 1, 2 or 3. Warning level 1 includes only default and high severity Level 2 includes medium severity. Level 2 is the default warning level 3 includes low severity vulnerabilities.
- **-x** Causes the default vulnerability databases (which are in the installation data directory, `/usr/local/lib` by default) to not be loaded.

When started, RATS will scan each file specified on the command line and produce a report when scanning is complete. What vulnerabilities are reported in the final report depend on the data contained in the vulnerability database or databases that are used and the warning level in use.

For each vulnerability, the list of files and line numbers where it occurred is given, followed by a brief description of the vulnerability and suggested action.

Reply With Quote

+ Reply to Thread

Quick Navigation **Network Tools** **Top**

« Previous Thread | Next Thread »

Tags for this Thread

[rats](#), [security analyst](#)  
[View Tag Cloud](#)



Posting Permissions

You may not post new threads

You may not post replies

You may not post attachments

You may not edit your posts

BB code is On

Smilies are On

[IMG] code is On

HTML code is On

Forum Rules

Contact Us

Network Analysis Community

Archive

Top

Links : Colasoft |Colasoft Australia|LoveMyTool|Protocolbase|Packet Sniffer|Free Network Tools|Network Monitor|network analyzer|network analysis|network traffic monitor|Free Cisco Lab