# SiVuS

*(**Si**P **Vu**lnerability **S**canner)*

**The VoIP Vulnerability Scanner**

# User Guide v1.07

www.vopsecurity.org

# Contents



# Figures

# 1 Introduction

SiVuS is the first publicly available vulnerability scanner for VoIP networks that use the SIP[1] protocol. If you are not familiar with SIP you can browse through the on-line tutorials that are listed at the end of this document or under the "*SIP Help*" tab in the SiVuS interface. The scanner provides several powerful features to verify the robustness and secure implementation of a SIP component. These features are described in the sections below.

SiVuS is used primarily by developers, administrators, network designers, managers and consultants to verify the robustness and security of their SIP implementations by generating the attacks that are included in the SiVuS database or by crafting their own SIP messages using the SIP Message generator.

The following figure depicts a simple network configuration which allows the SiVuS scanner to identify targets and perform vulnerability analysis.

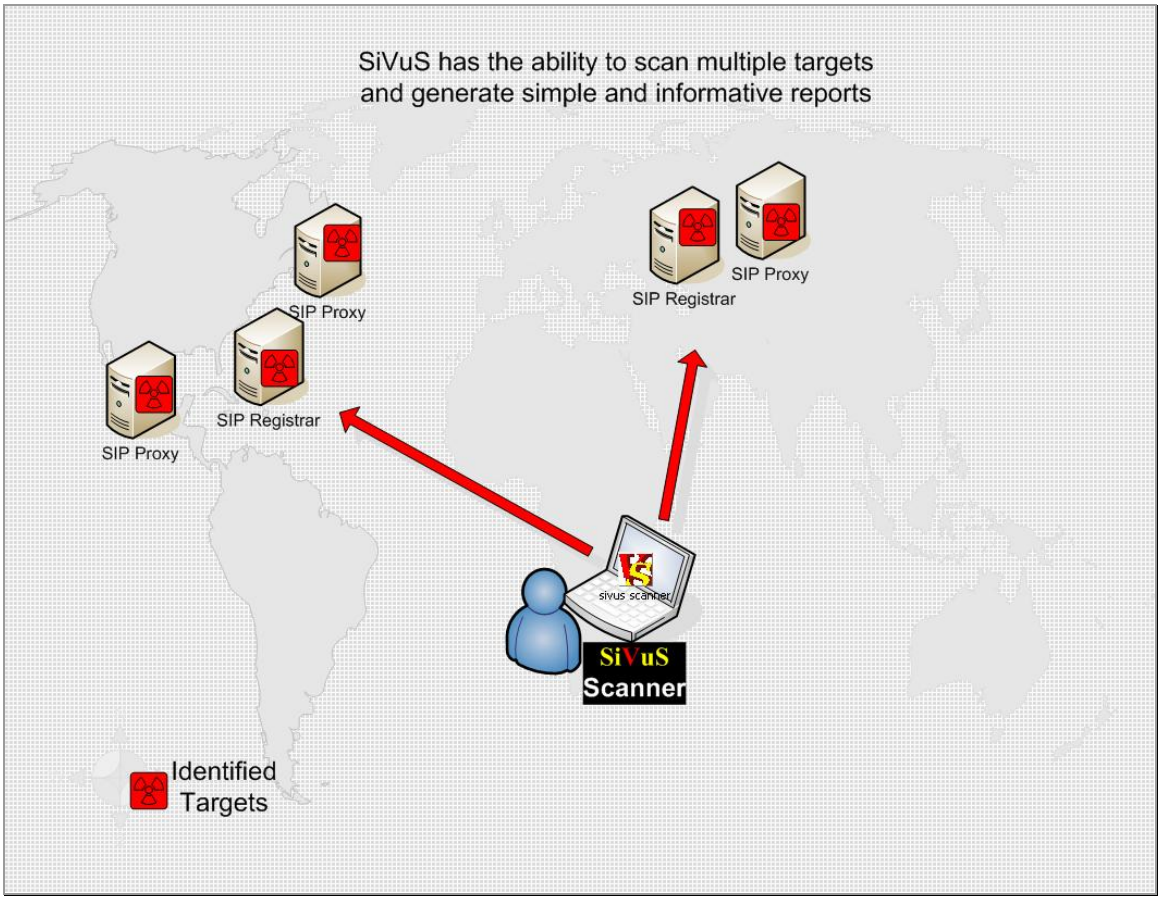



**Figure 1 - Simple scanning configuration**

[1] Session Initiation Protocol, RFC 3261

The user has the ability to supply the scanner with various IP address ranges where targets can be identified for further analysis. The user has also the ability to generate specific SIP messages (using the SIP message generator) that can be used to demonstrate a distinct vulnerability.

The following sections describe the SiVuS features and functionality.

# 2 SiVuS Features and Functionality

The SiVuS scanner provides powerful features that allow administrators, developers and consultants to verify the robustness and secure implementation of SIP components such as Proxies, Registrars or phones (hard or soft). The following paragraphs provide additional detail on the functionality and features:

- **SIP Message generator** : it can be used to send various types of messages to a SIP component including SDP content. This feature can be used to test specific issues with SIP or generate various attacks for demonstration purposes (e.g. DoS, registration masquerading).

- **SIP component discovery**: it scans a range of IP addresses to identify hosts which use the SIP protocol and can be used as targets for further analysis. Note, that there is an option in the configuration scanner which allows preliminary discovery of targets prior to an actual scan. The discovery interface is typically used as a precursor to a scan to ensure that the appropriate targets should be scanned. Other uses of this feature are possible.

- **SIP vulnerability Scanner**: The scanner provides flexible configuration of several options which can be used to verify the robustness and security of a SIP implementation.

    - Checks that are performed:
        - Analysis of the SIP message headers to identify vulnerabilities such as Buffer overflows or denial of service attacks. These checks can be selected and configured with variable values, by the user.
        - Authentication of signaling messages by the SIP component under analysis.
        - Authentication of registration requests.
        - Inspection for secure communications (SIPS) and encryption capabilities
    - Reporting:
        - At the moment the scanner provides a user friendly report using HTML. Later versions of the scanner will support multiple arrangements and views of the data collected after a scan including maintaining a history of scanning sessions.
        - The user has also the ability to save messages from the activity log that are generated during a scanning session for later analysis.

- **SIP Help:** the SiVuS interface provides quick help on common topics that may be useful to a user while performing an assessment. The SIP help provides the latest version of the SIP RFC 3261, sample SIP messages that can help a novice user to construct SIP messages through the SIP message generator, and references to online resources that discuss SIP including tutorials.

# 3 Installation

Installation and execution Requirements:

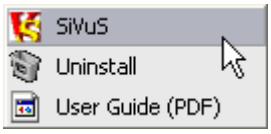
- Java JDK 1.4+
- RAM Memory : minimum 56MB
- Hard disk: 2.40 MB

The following steps describe the installation:

- Run the Install Wizard (sivus-1.07.exe) and follow the steps
- If you experience any problems send us an email sivus@vopsecurity.org or post a message on the mailing list or SIVuS forum on the www.vopsecurity.org website.

# 4 Operation

You can start the SiVuS software from the SiVuS group icon.




The following sections provide a description for configuring the features and performing a scan.

## *4.1 SIP Component Discovery*

Typically the first operation that you may perform is to identify network elements which use SIP. The SIP Component Discovery utility provides an easy way to identify hosts which use the SIP protocol (including SIPS) and can be used as targets in the scanner's configuration.

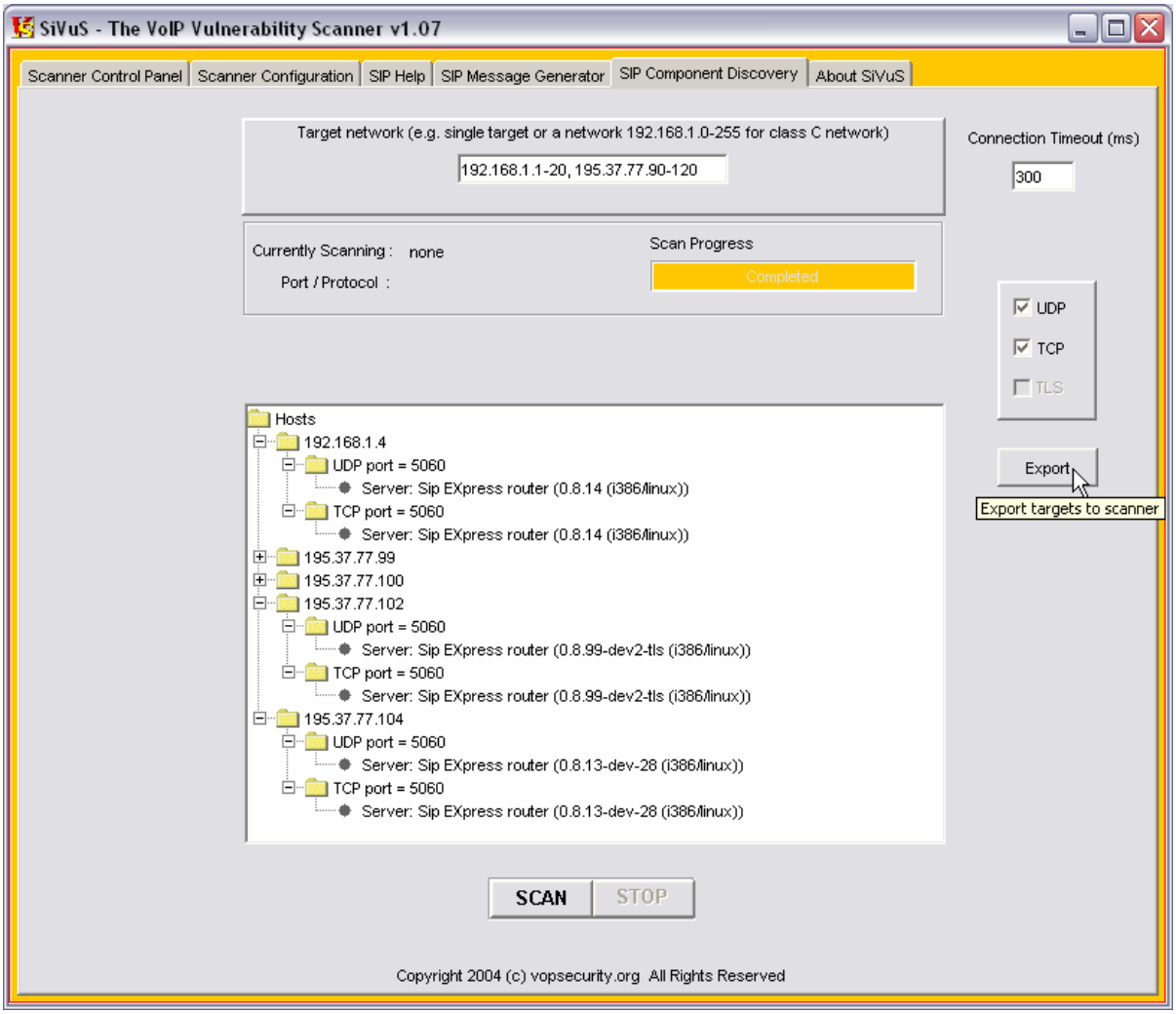



**Figure 2 - Discovery Scanner Example**

The format in the target network field is similar to the scanner's configuration which is as follows:

- 192.168.1.3 – a **single IP** address to scan.
- 192.168.1.3**,**192.168.1.4**,**192.168.5.10 – scan **three IP** addresses (note that each address is separated by a comma)
- 192.168.1.1-255 – scan the **entire C-class**
- 192.168.1.13-15 – scan hosts between 13 and 15 inclusively
- 192.168.2-10.1-5 – scan the B class between subnets 2 and 10 and hosts 1 through 5

The user has the ability to alter the connection timeout value in order to adjust to network performance requirements.

The utility allows scanning for UDP, TCP and TLS[2] ports that are typically used by SIP components.

Once targets have been identified you can "export" them to the scanner's configuration panel by clicking on the "**Export**" button.

## 4.2 Automated Scanning

In order to perform an automated scanning you need to populate the "*Scanner Configuration*" tab with the appropriate information and then control the scanning session from the "*Scanner Control Panel*" tab.

The following two sections discuss each one.

### 4.2.1 Scanner Configuration

The scanner configuration tab allows you to select the appropriate options to perform a scan.

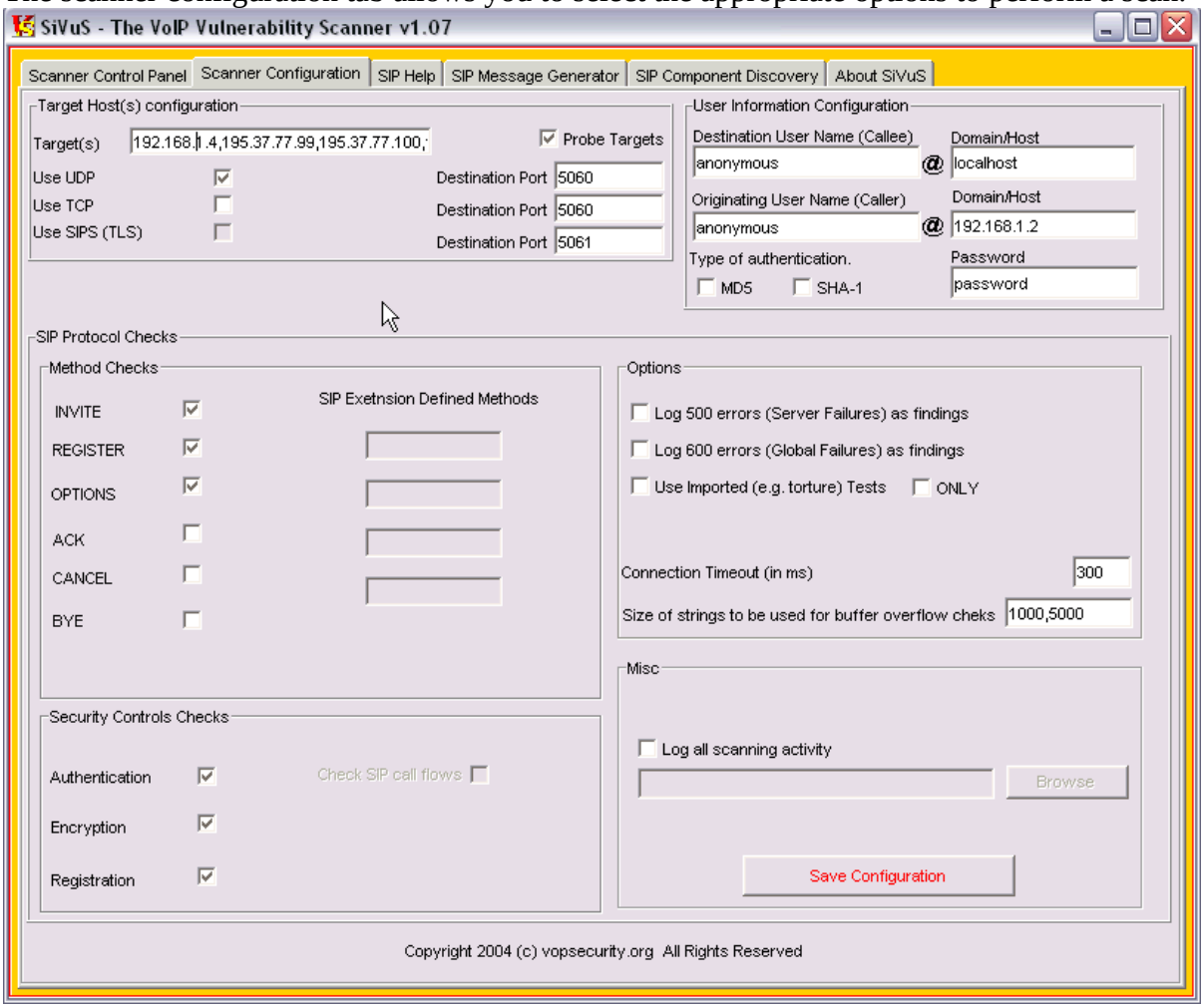



**Figure 3 - SiVuS Scanner Configuration Menu**

[2] The TLS option was disabled temporarily in this version due to re-development of the code.

There are various configurations options which are discussed in the sections below.

### 4.2.1.1 Target host configuration

In order to initiate a scan you need to provide a set of IP addresses or a single IP address of a host which is considered to be the target. The format of the IP addresses is as follows:

- 192.168.1.3 – a **single IP** address to scan.
- 192.168.1.3**,**192.168.1.4**,**192.168.5.10 – scan **three IP** addresses (note that each address is separated by a comma)
- 192.168.1.1-255 – scan the **entire C-class**
- 192.168.1.13-15 – scan hosts between 13 and 15 inclusively
- 192.168.2-10.1-5 – scan the B class between subnets 2 and 10 and hosts 1 through 5

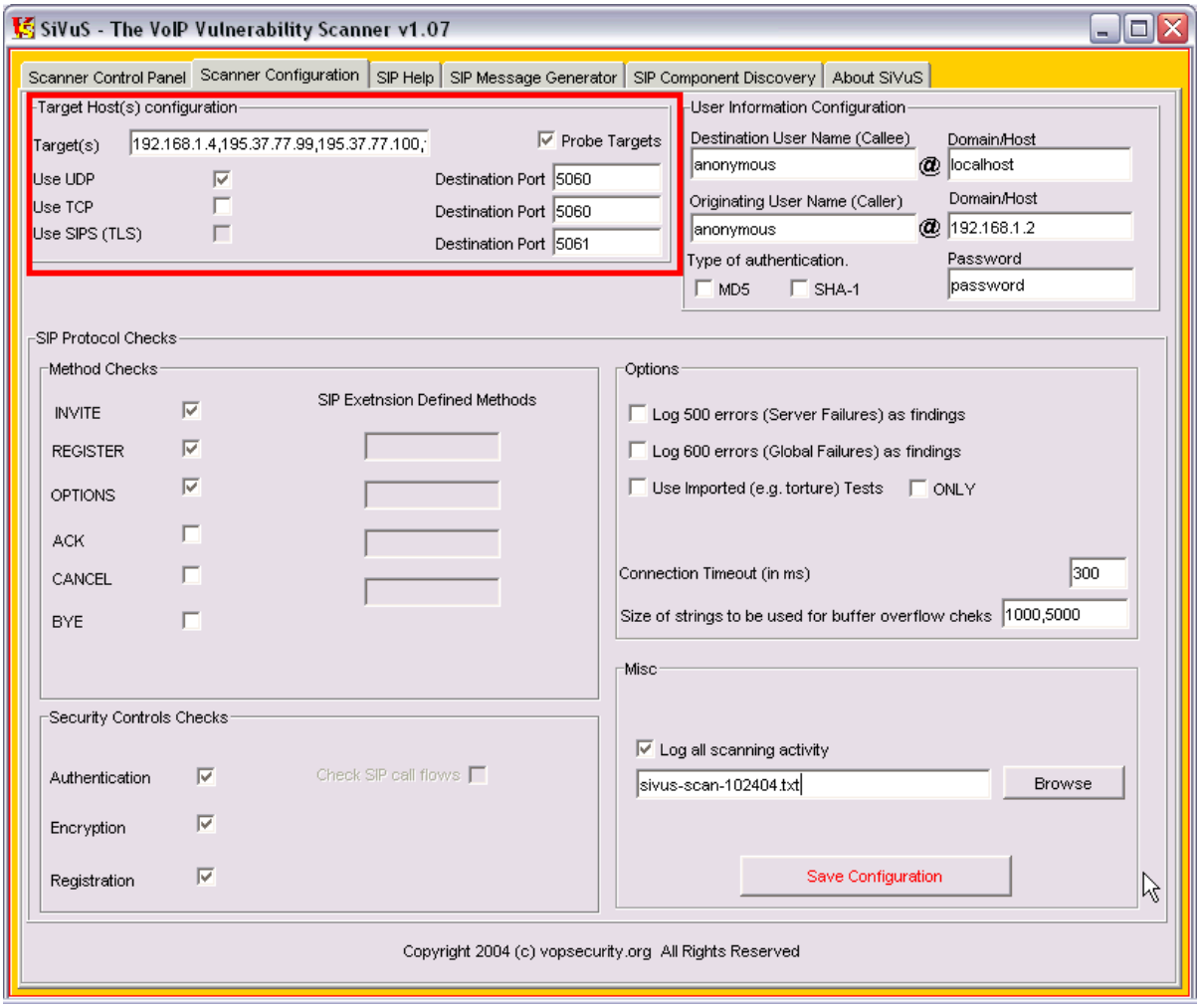



**Figure 4 - Configuring targets**

The scanner can perform vulnerability scans using UDP (the default medium for SIP), TCP and TLS[3] for SIPS.

The *Probe-Targets* option helps verify that the target host is a SIP component prior to initiating a scan against it. The ability to identify SIP components can be achieved by using the SIP Component Discovery function.

Furthermore, the user can change the server's destination port for each respective protocol (UDP,TCP and TLS). The default values for each protocol are pre-populated.

### 4.2.1.2 User information Configuration

The scanner's configuration panel gives you the ability to populate the source and destination user information, that will be used in the messages to be generated during the scan session.

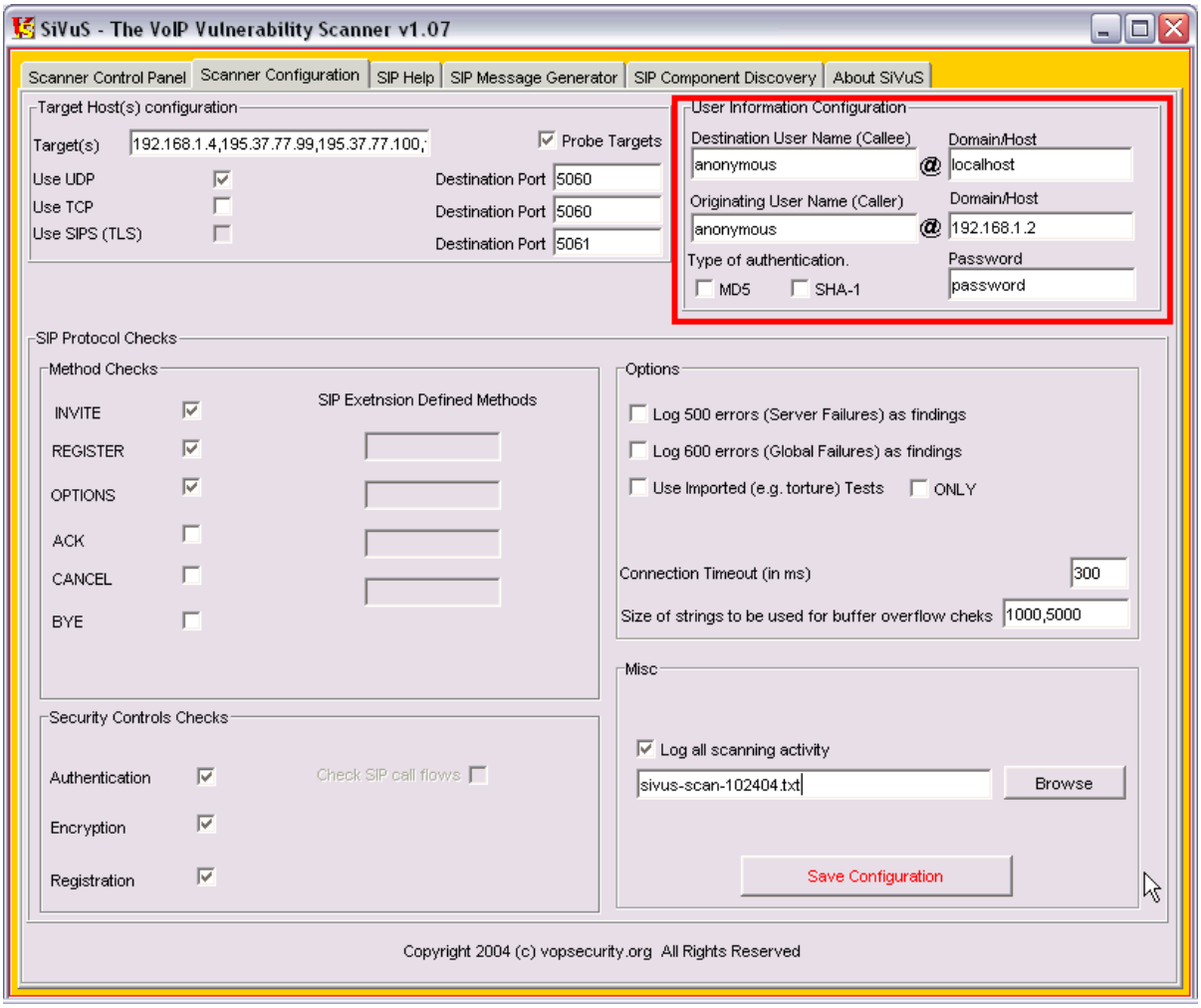



**Figure 5 - User Information Configuration**

[3] The TLS option was disabled temporarily in this version due to re-development of the code.

It is recommended that a test user is defined as the recipient of these messages (calls) in order to minimize user annoyance in a production network.

The *Destination User Name* field identifies the user that will receive the messages generated by the scanner. The default values can be used but in certain cases it may be required to configure an existing user name in order to observe the behavior of the target host based on the test messages generated.

The *Destination Domain/Host* field identifies the target domain that the scanner's messages should contain. The same logic can be used as the previous description regarding observing the behavior of the target component.

The *Originating User Name* field identifies the user that supposedly is originating the messages. The default values can be used but in certain cases it may be required to configure an existing user name in order to authenticate messages if required and observe the behavior of the target host based on the test messages generated. You will need to populate this field, along with the *Password* field, with a legitimate user name in order to test SIPUA's that require authentication.

The *Originating Domain/Host* field identifies the domain that the messages are supposedly generated. This is not a required field but the same logic as the previous fields (i.e. *Destination User Name*) applies.

The *Type-of-Authentication* option provides the ability to indicate what type of authentication digest should be used, if the target hosts are using authentication prior to processing any messages. Typically, MD5 is the common choice of message digest algorithm used, but the SHA-1 is also provided in case there are proprietary implementations of SIP stacks that may use this digest algorithm.

### 4.2.1.3 SIP Checks

The following sections discuss the various SIP checks that are available in this version of the scanner.

#### *4.2.1.3.1 Method Checks*

The user can select which methods are to be tested by selecting the desired methods within the *Method-Checks* section.

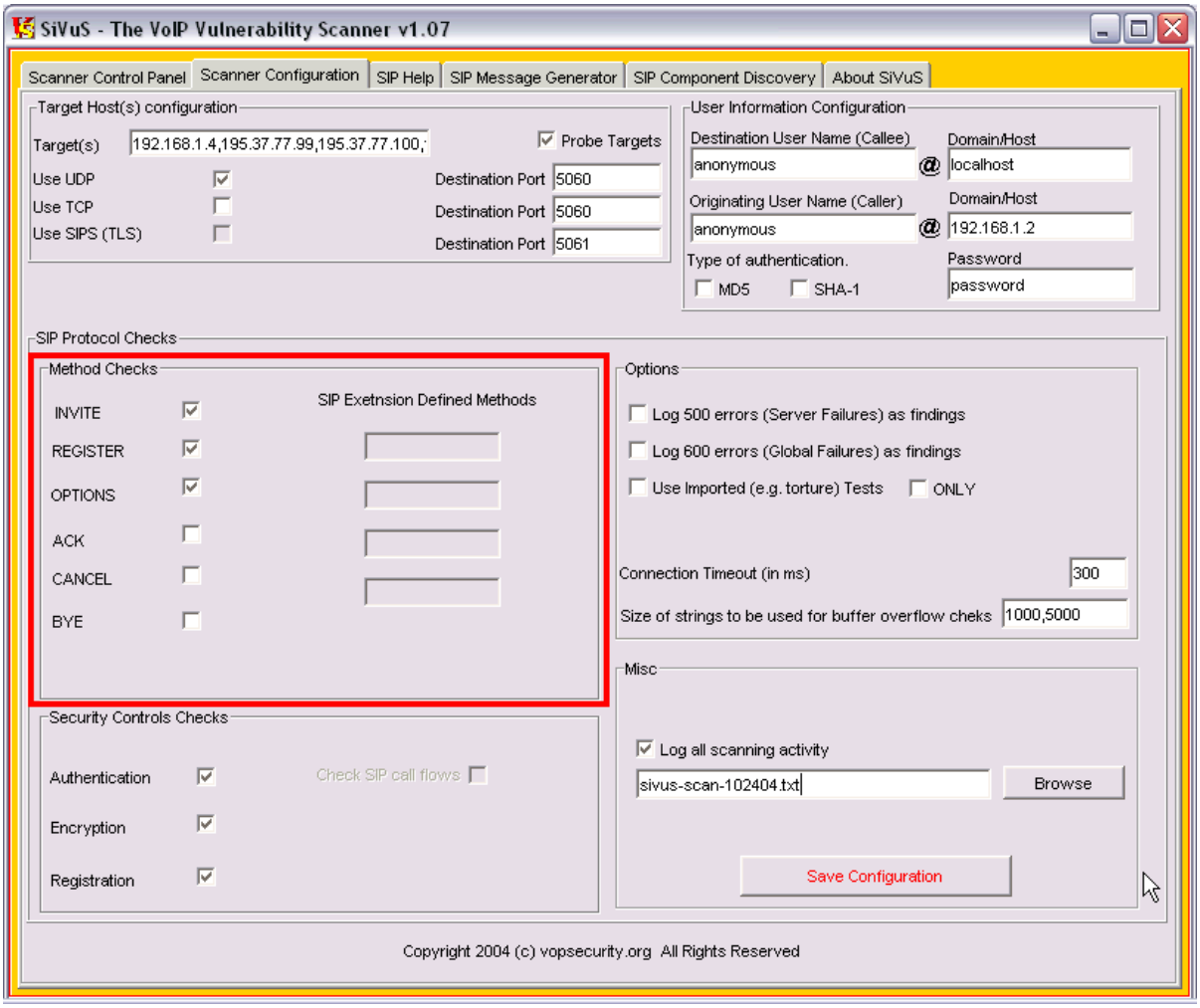



**Figure 6 - Methods-Checks**

The scanner also provides the ability to incorporate additional methods that may be defined in other SIP extensions.

Each method is tested for various vulnerabilities (e.g. buffer overflows, malformed messages) using combinations of the available header fields and parameters (username, Tag, Call-ID, etc.). The size of the strings for buffer overflow checks is defined in the *Options* section.

### *4.2.1.3.2 Security Controls Checks*

The scanner also checks for the ability of the target components to perform the following:

- authentication of SIP messages
- registrations and
- encryption capabilities.

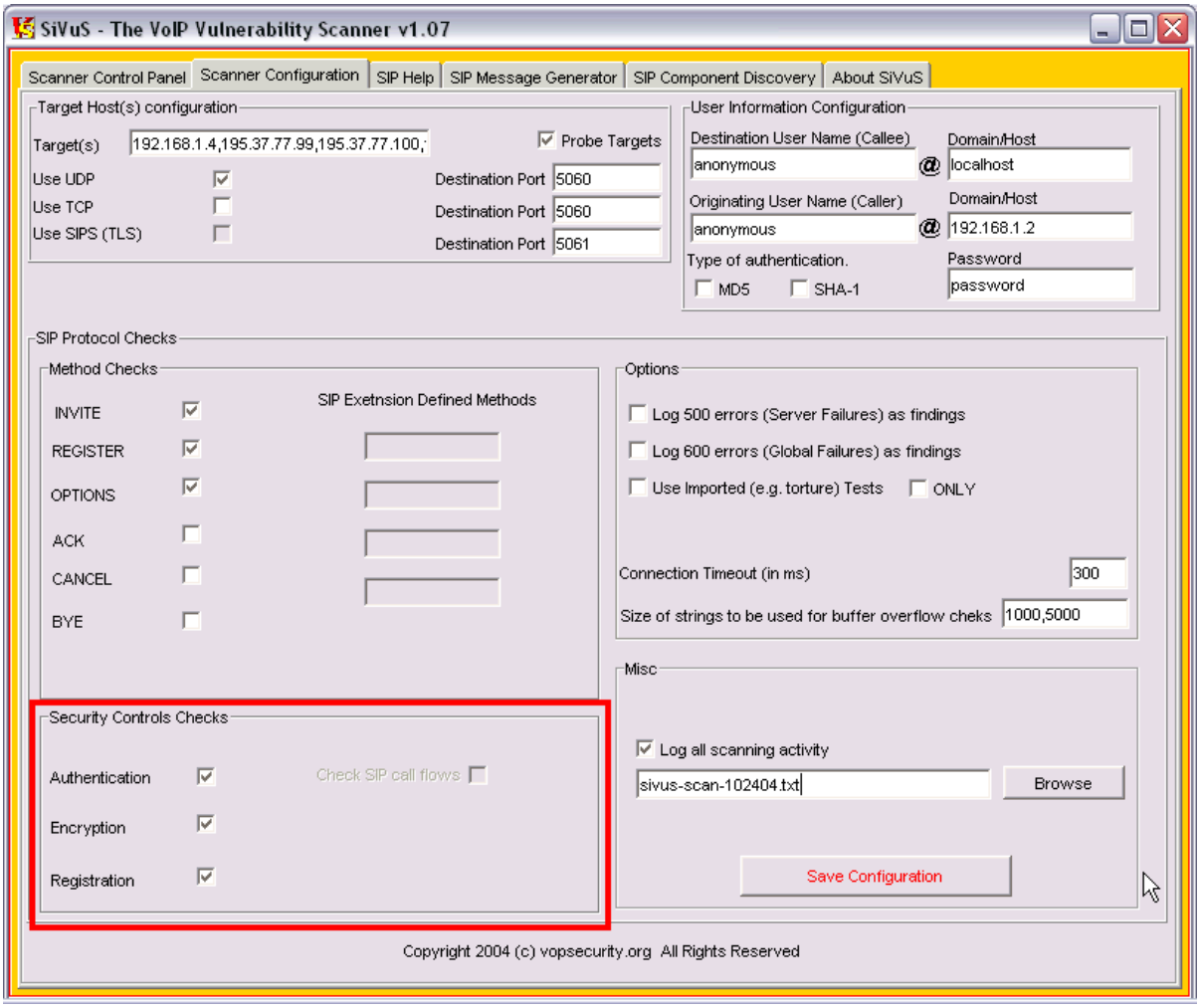



**Figure 7 - Security Controls Checks**

### *4.2.1.3.3 Options*

#### 4.2.1.3.3.1 Logging Global and Server failures

If you like to know when checks generate *Global* or *Server* errors select the respective checkbox (*Log 500 errors* and *Log 600 errors*) . In certain cases, vulnerability checks may cause a Global or Server error which may have significant impact to the health of the target component. By default these two options are disabled.

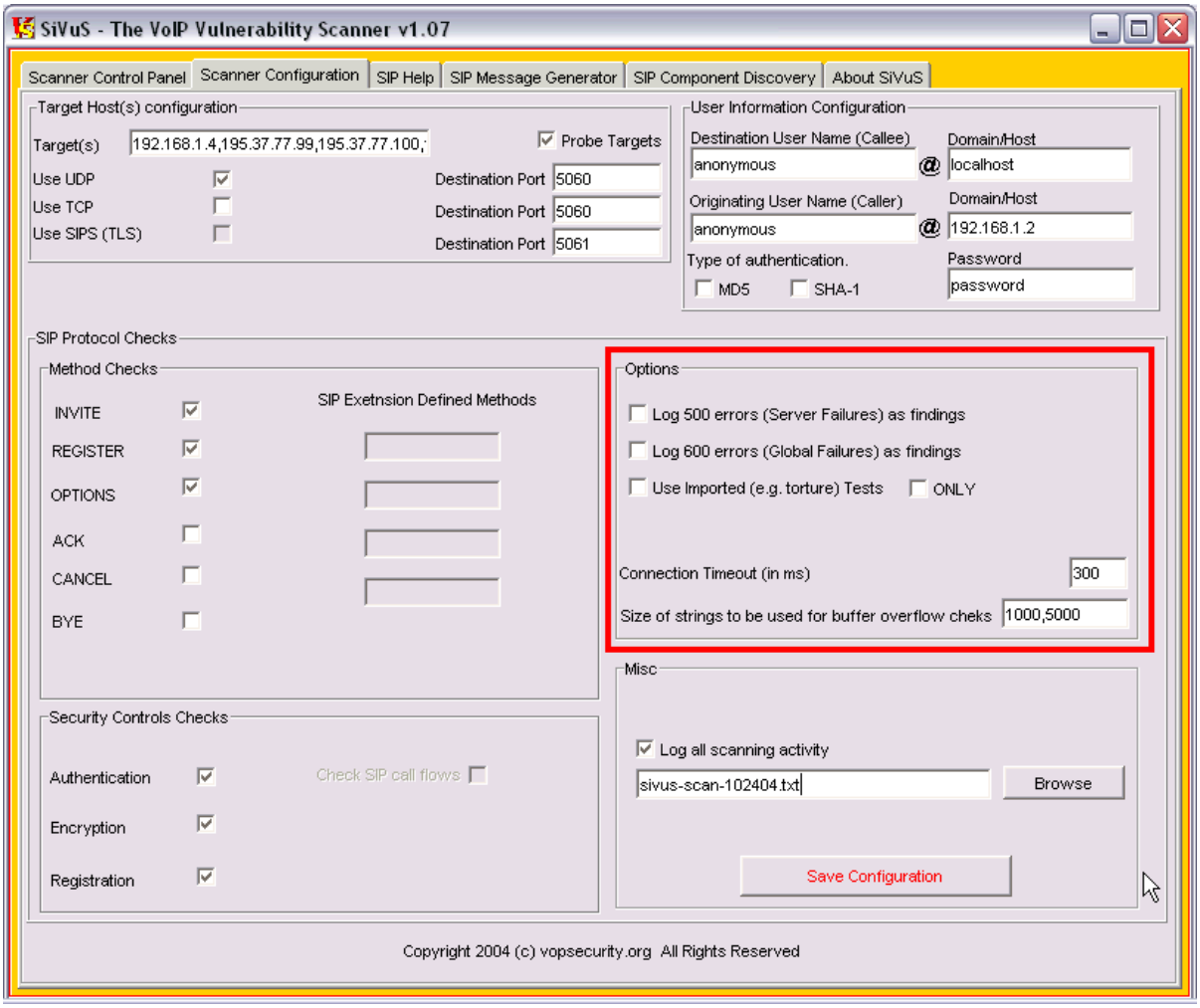



**Figure 8 – Scanner Configuration Options**

#### 4.2.1.3.3.2 Using imported checks (e.g. torture checks)

You can import Torture checks (from the Control Panel) and have the scanner send the checks to specified targets. The scanner provides the option to use *ONLY* imported checks which can be useful when testing for SIP compliance. NOTE: at this time[4] this option will not generate any reports. You have to use a network analyzer (e.g. ethereal) to monitor the responses.

In addition, the user has the ability to alter the *Connection Timeout* value in order to adjust to network performance requirements.

#### 4.2.1.3.3.3 Configuring Buffer Overflow check size

[4] There are plans to integrate an analysis module to recognize responses when torture tests are used.

The user can specify the *Size* of the strings that should be generated in order to check for buffer overflows, malformed messages and potential Denial of Service.

NOTE: we have discovered that the Windows OS'es have a limitation on sending oversized packets of 50,000 characters. You may receive an error if you attempt to generate such a large message.

### *4.2.1.3.4 Misc*

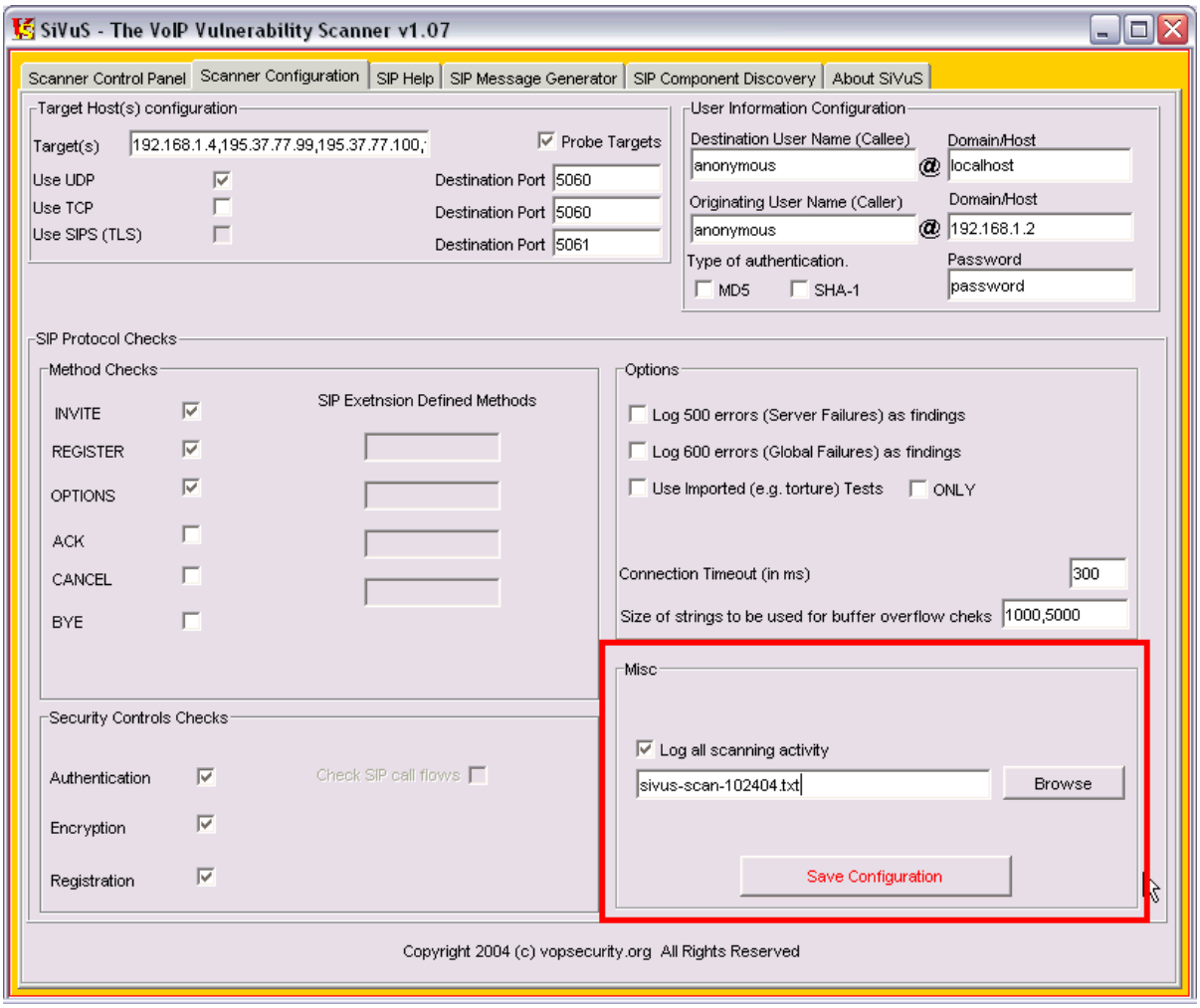



**Figure 9 - Saving scanner configuration and logging scanner activity**

#### 4.2.1.3.4.1 Logging scanning activity

You can log all the messages send and received during a scanning section by selecting the *Log all scanning activity* box.

#### 4.2.1.3.4.2 Saving scanner configuration

Click on *Save Configuration* to save the current configuration to be used at a later time by selecting it from the scanner's Control Panel..

### 4.2.2 Scanner Control Panel

The scanner control panel provides the ability to initiate a scan, stop, monitor the progress of a scan and generate reports.

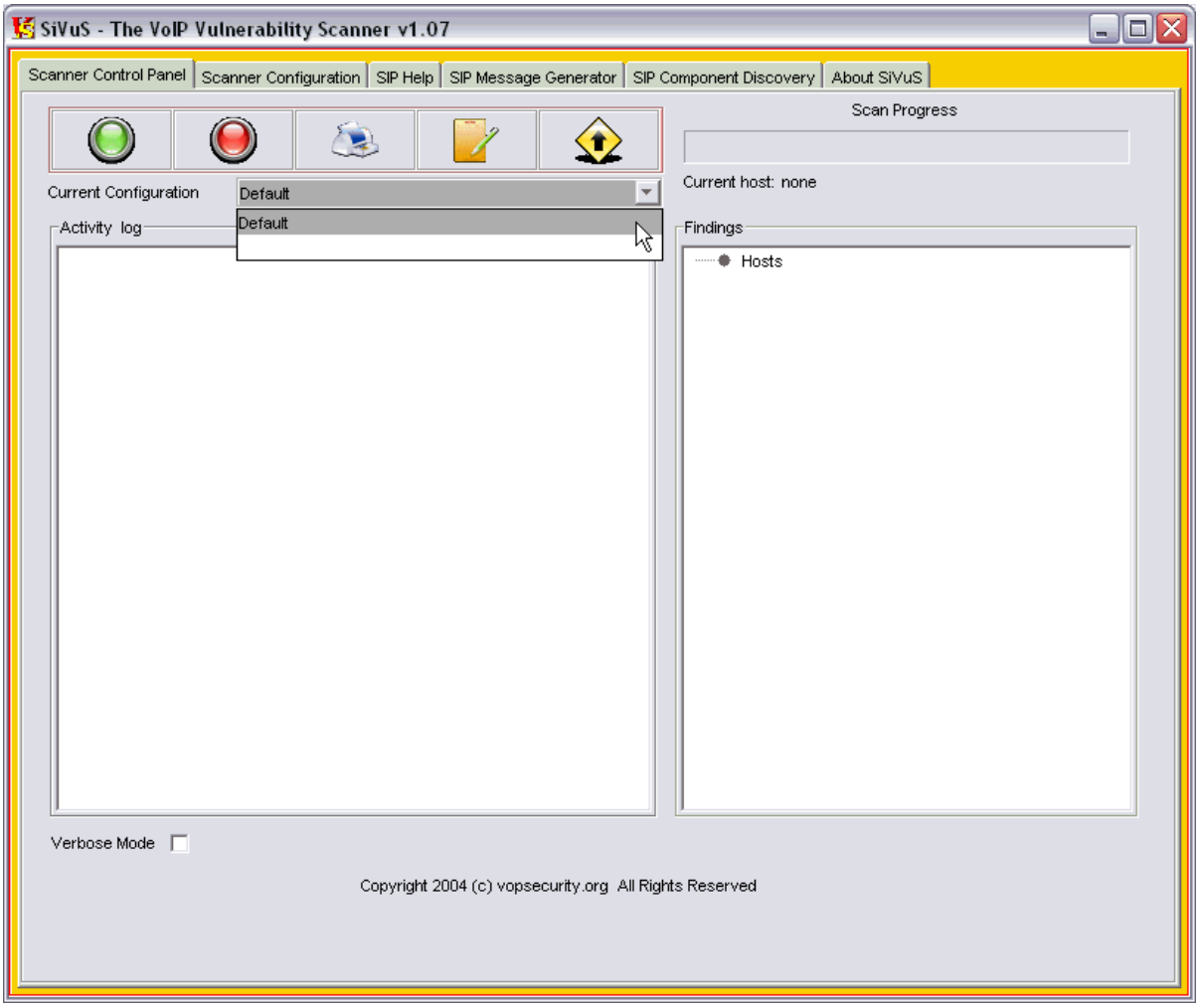



**Figure 10 – Scanner Control Panel**

The scanner window provides the user with the ability to monitor the progress of the scanner and messages sent and received (by checking the *Verbose-Mode* check box at the lower left corner of the panel). In addition and vulnerabilities that are identified during the scan are listed under the *Findings* panel in tree structure.

The *Current Configuration* dropdown field allows the user to select which configuration to use for a scanning session. This ability can be useful in various scenarios. For example you

can use same configuration to scan multiple networks and maintain a consistency of the type of checks that are performed or maintain a historical record of the scanning session and the checks that were used.

#### 4.2.2.1 Activity Log

You can save the activity log window by clocking on the "*Activity Log*" button.

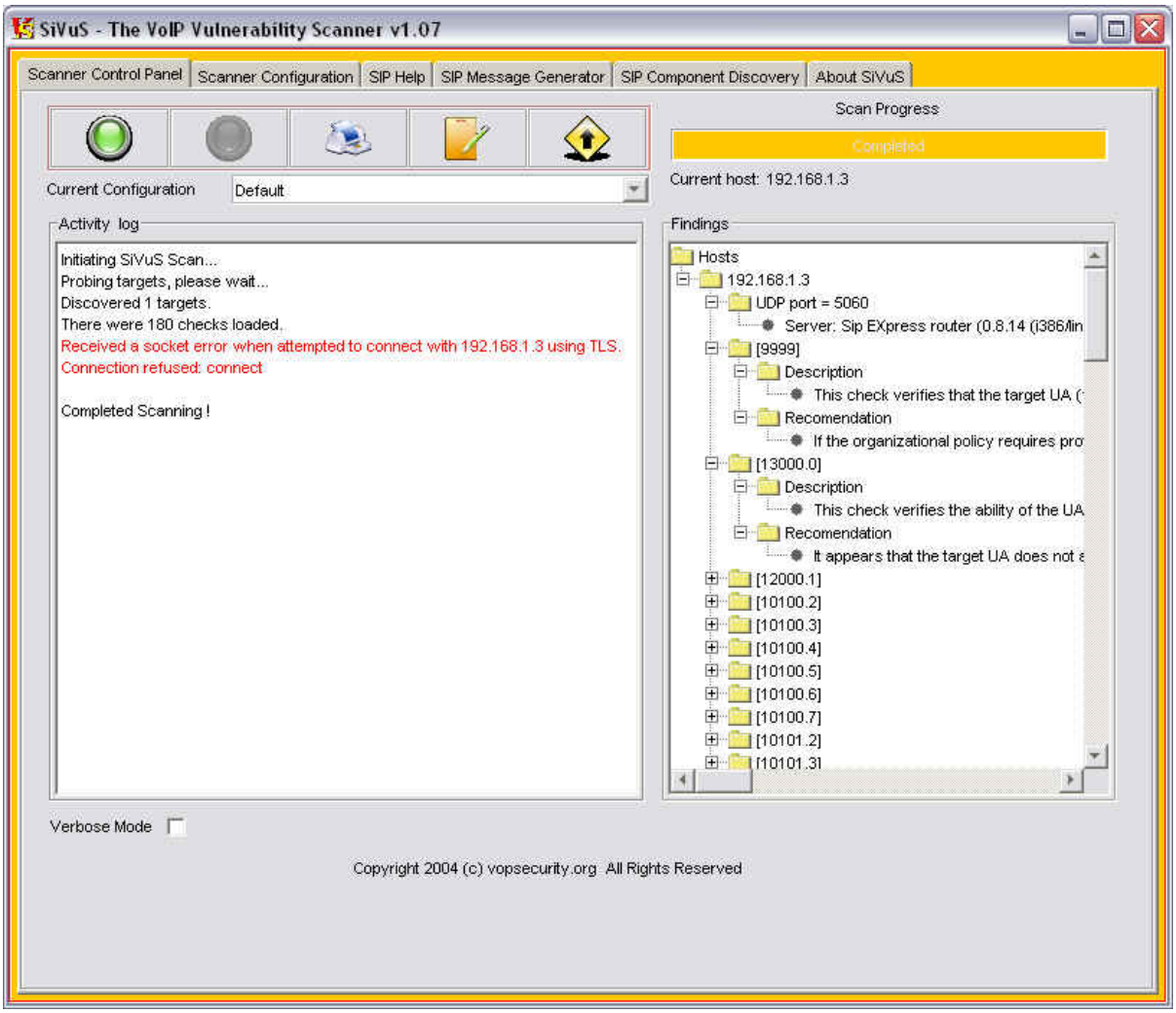
#### 4.2.2.2 Importing Checks (e.g. Torture checks)

You can import checks by clicking on the "*Import Checks*" button and have the scanner send the checks to specified targets. The scanner provides the option to use *ONLY* imported checks (selectable from the configuration panel) which can be useful when testing for SIP compliance. NOTE: at this time[5] this option will not generate any reports. You have to use a network analyzer (e.g. ethereal) to monitor the responses.

#### 4.2.2.3 Findings window

The Findings window provides a preliminary display of the findings that the scanner has identified.

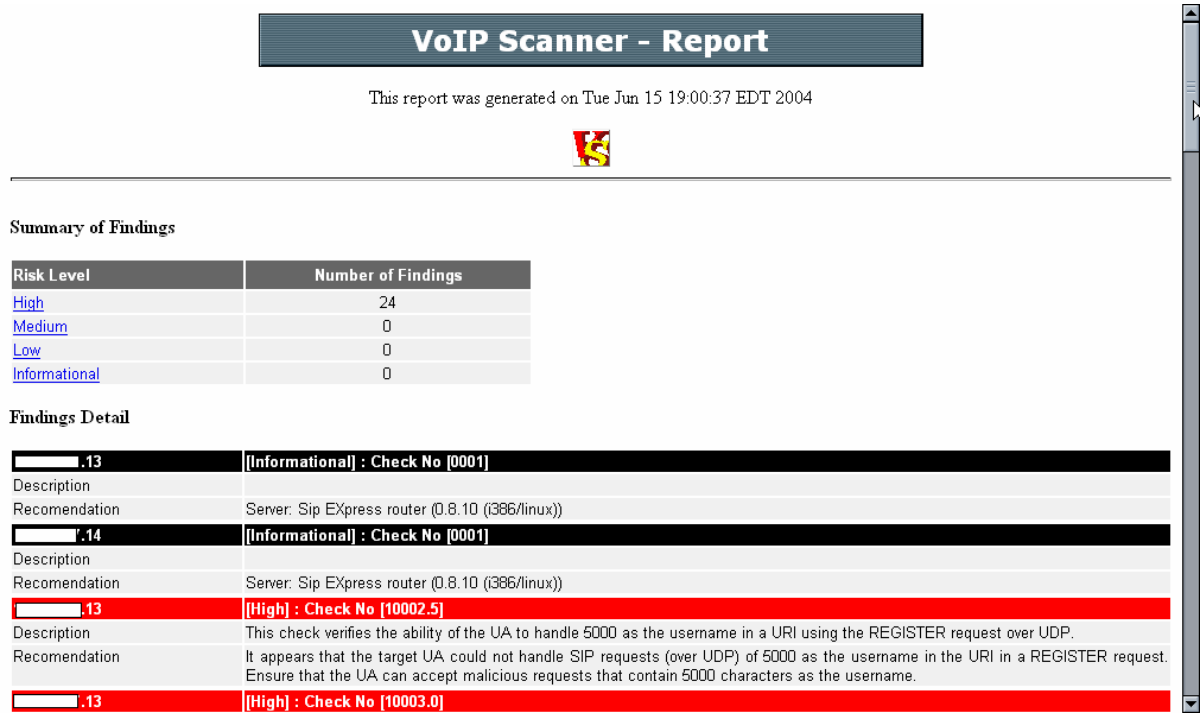
[5] There are plans to integrate an analysis module to recognize responses when torture tests are used.




### 4.2.3 Generating a report

Once you have completed (or stopped) a scan, you can click on the "*printer*"  icon to generate a report. The report will be stored in a subdirectory "*Reports*" under the scanner's directory.

The following is a sample report (the first three octets of the IP address have been purposefully obfuscated).



VoIP Scanner - Report

This report was generated on Tue Jun 15 19:00:37 EDT 2004

Summary of Findings

| Risk Level | Number of Findings |
|---|---|
| High | 24 |
| Medium | 0 |
| Low | 0 |
| Informational | 0 |

Findings Detail

| | |
|---|---|
| [redacted].13 | [Informational] : Check No [0001] |
| Description | |
| Recomendation | Server: Sip EXpress router (0.8.10 (i386/linux)) |
| [redacted].14 | [Informational] : Check No [0001] |
| Description | |
| Recomendation | Server: Sip EXpress router (0.8.10 (i386/linux)) |
| [redacted].13 | [High] : Check No [10002.5] |
| Description | This check verifies the ability of the UA to handle 5000 as the username in a URI using the REGISTER request over UDP. |
| Recomendation | It appears that the target UA could not handle SIP requests (over UDP) of 5000 as the username in the URI in a REGISTER request. Ensure that the UA can accept malicious requests that contain 5000 characters as the username. |
| [redacted].13 | [High] : Check No [10003.0] |

**Figure 11 - Sample report**

## *4.3 SIP Message Generator*

The SIP Message Generator provides a flexible way to generate single SIP messages based on the user's parameters.

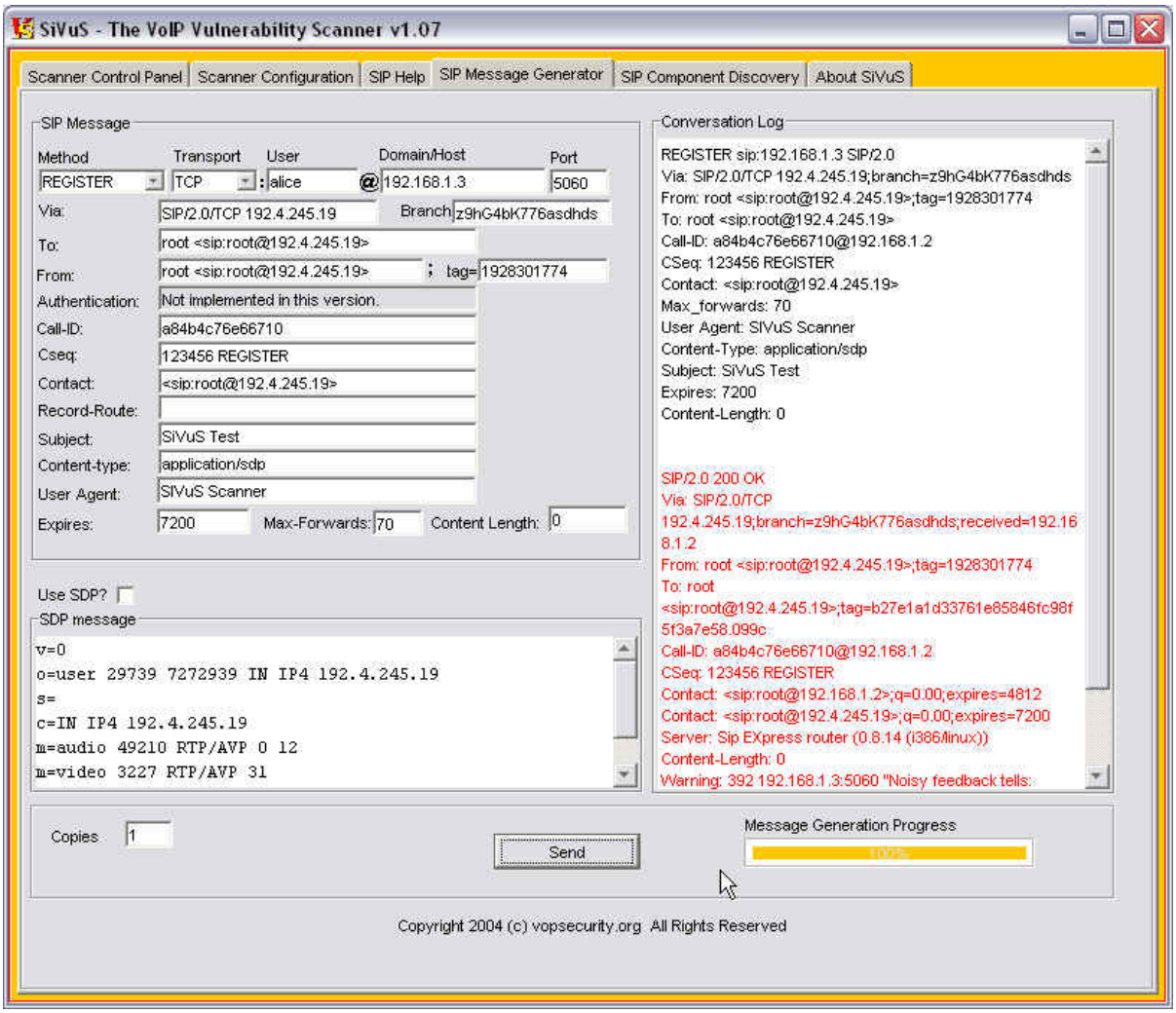



**Figure 12 - SIP Message Generator**

The requests (in black) and responses from the server (in red) are displayed on the *Conversation Log* window.

The required fields for a SIP message are emphasized in the following example:

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK77ds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
```

The *SIP Message Generator* can generate messages with the following options:

- Methods: INVITE, REGISTER, CANCEL, OPTIONS, BYE and ACK by selecting the drop down *method* tray.

- Transport : TCP, UDP or TLS (for SIPS) by selecting the drop down *transport* tray.

- User : the remote *user* (callee) which is to receive the message.

- The *Target Domain/Host* where the user may be residing

- The destination *port*, which by default is 5060 for SIP and 5061 for SIPS.

- The body of the SIP Message can include several other fields which are described in detail in the SIP RFC 3261 and other literature available on the Internet (see Appendix-A for additional references). The *SIP Message Generator* provides the most commonly used headers to generate a message and interact with another SIP component.

- Finally, the *SIP Message Generator* has the option to generate multiple copies of the same message by specifying the number of copies, by populating the *Copies* field located at the lower left corner of the interface. This feature can be used to load a proxy server with multiple messages in order to identify it's robustness and study the behavior of potential service degradation.

In addition, the user can define an SDP message to be included in the SIP message. The changes in the SDP message section have to be manually defined. The SIP Message Generator will parse and reformat the SDP headers before they are sent to the target host. So the SDP section can include any type of data that the user can enter (e.g. long string of characters) and it will be sent "as-is" within the SIP message.

The SIP Message Generator interface provides description of the values that a field can have. The following example illustrates this when the user places the cursor over the "content-length" field.

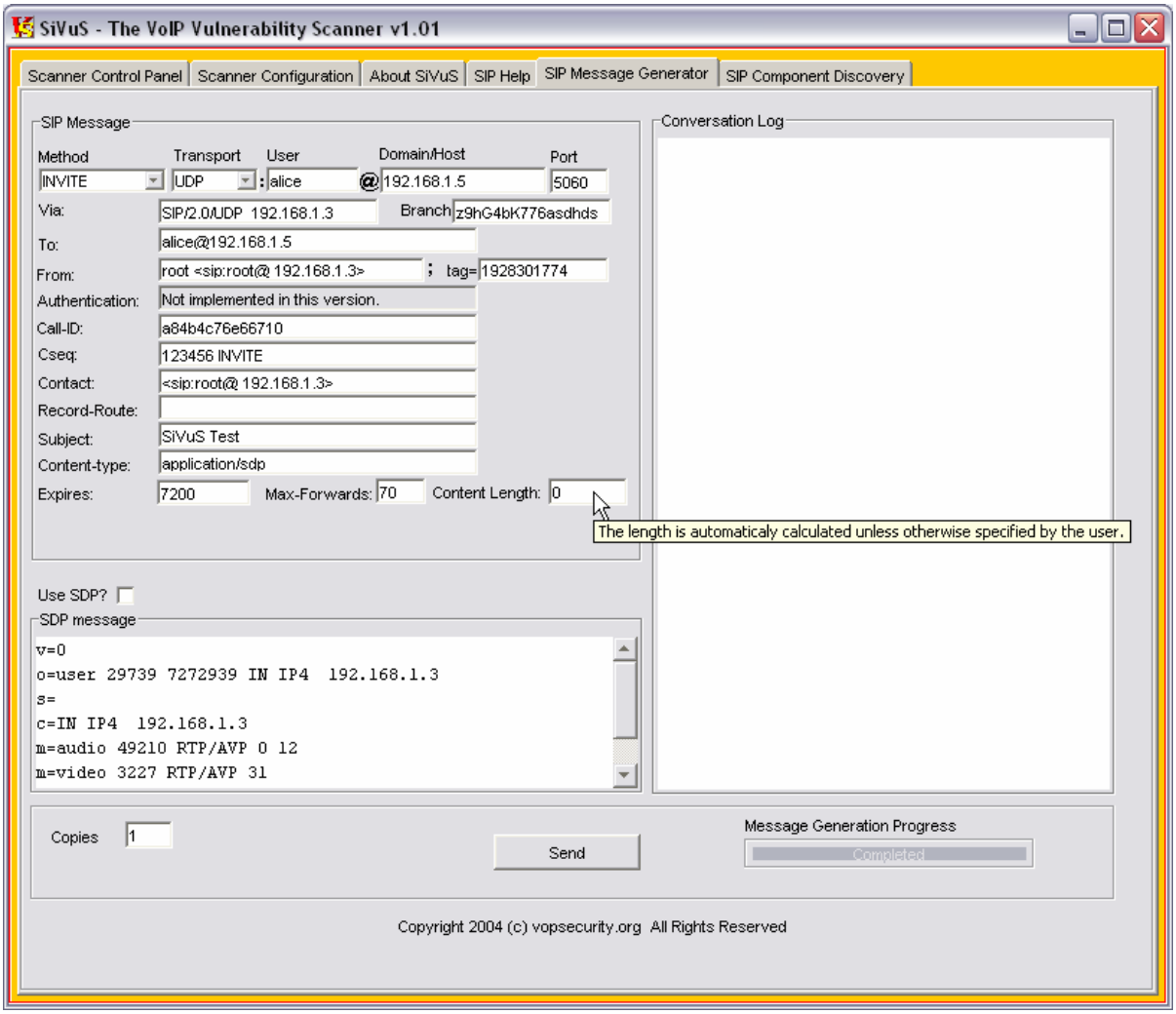



**Figure 13 - SIP Message Generator tool tips**

The following image depicts an example of a SIP **INVITE** message that is sent to a SIP proxy, from "*root@192.168.1.3*", requesting to contact user "*alice@ 192.168.1.5*".

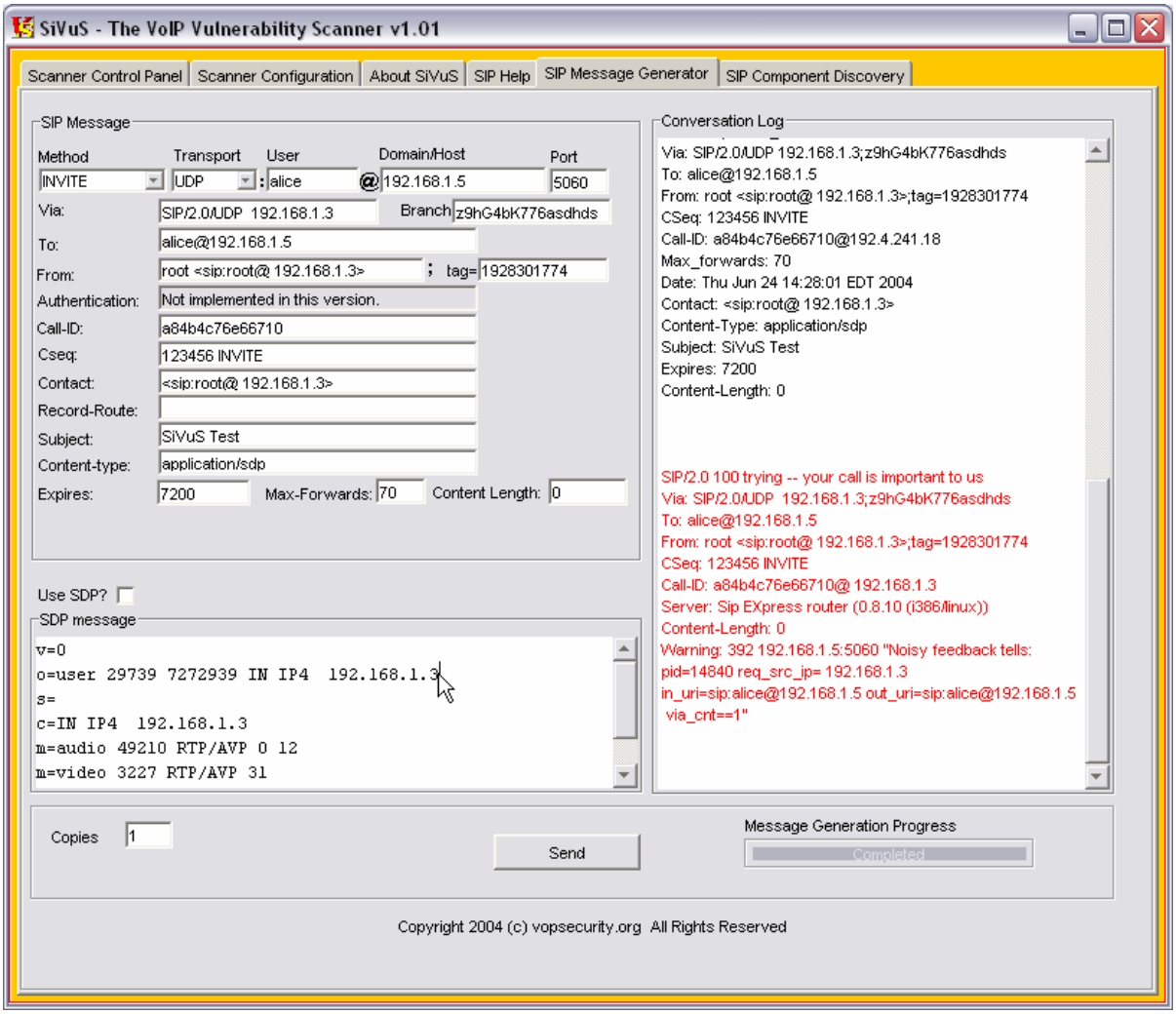



**Figure 14 - SIP INVITE example**

Note that the SDP portion of the message is automatically populated with the necessary information (e.g. source IP address) to match the SIP headers. This information can also be changed by the user as desired, prior to sending the SIP message.

The user's request in black text and the server's response, in red, are displayed in the conversation log window.

# 5 SIP Help

The SiVuS interface provides quick help on common topics that may be useful to a user while performing an assessment. The SIP help provides the latest version of the SIP RFC 3261, sample SIP messages that can help a novice user to construct SIP messages through the SIP message generator, and references to online resources that discuss SIP including tutorials.

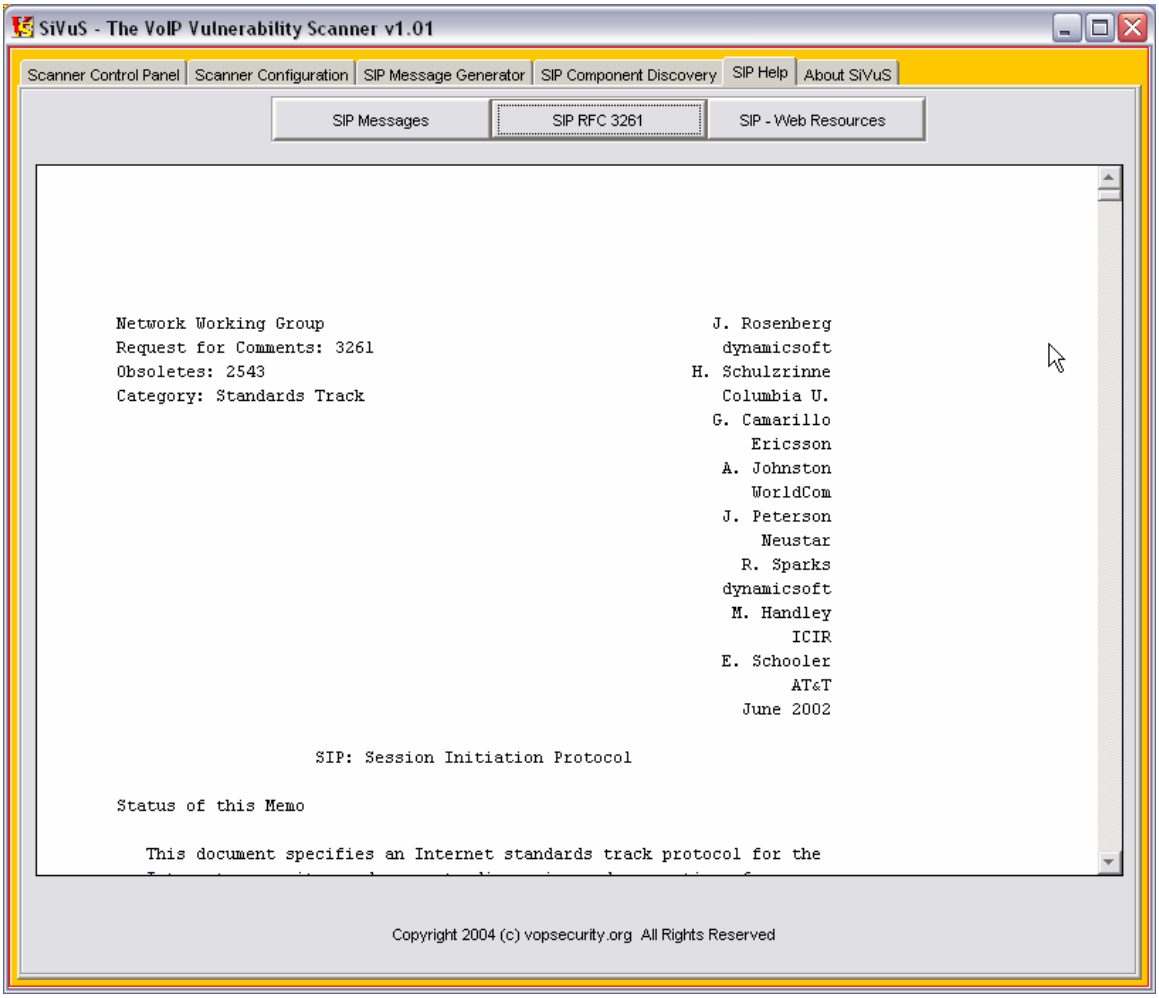



**Figure 15 - SIP help tab**

# Appendix A – References and Links

- www.vopsecurity.org , a web portal which captures security issues regarding Voice over packet networks or NGN networks.
- SIP FAQ http://www.cs.columbia.edu/sip/faq/
- IP Telephonly with SIP - www.iptel.org/sip/
- SIP Tutorials
    - The Session Initiation Protocol (SIP) http://www.cs.columbia.edu/~hgs/teaching/ais/slides/sip_long.pdf
    - SIP and the new network communications model http://www.webtorials.com/main/resource/papers/nortel/paper19.htm