SWP-SMTP v1.0
User Manual

(Proxy for Use with the
SMTP Protocol)

San José, Costa Rica 2004

Contents

Introduction

This user manual is presented as a guide for those system administrators that wish to install and configure SWP-SMTP, the proxy program for use with the SMTP protocol that is part of the system for detection and tagging of unsolicited or undesired e-mail or spam known as SpamWarn, which denotes the system or set of programs and not a particular program.

This manual is divided in three parts: Overview, Installation and Configuration.

An brief overview explaining how the proxy works is given in the first section.

The second part deals with topics such as the ways in which the SWP-SMTP program can be obtained and instructions for its installation in the selected platform.

In the third and last part, we explain the configuration parameters of the proxy and how they alter its behavior. The different values that these parameters are given, as well as the expected outcome of their use.

Typographic Conventions

The following typographic conventions are used in the scope of this document when denoting certain syntactic elements:

`Code` `Code`	This fixed-size font is used to denote file content samples, inputs or outputs of the system, commands, e-mail samples, etc.
Italics	Italics are used to highlight some contents inside the text.
Bold	And bold to denote reserved words used within the text itself.

```
CLI> COM
SRV> ANSWER
CLI> COM PAR
SRV> Line 1
SRV> Line 2
SRV> .
CLI>
```

Dialogs between the client and the server are shown in this way, in which the client commands are indicated with `CLI>` and the server responses are indicated with `SRV>`. Each command can have zero parameters (as in `CLI> COM`), or one parameter (as in `CLI> COM PAR`). Dialogs are alternating, that is, every client command will generate a response and the client must wait until a complete server response is received before sending a new command. Furthermore, the server is forced to generate a response that in turn allows the client to know the result of the last command, either successful or resulting in an error condition. Some client commands and server responses are made up of several lines and the end of the command or the response is given by a line with the hexadecimal ASCII code sequence `<2E><0D><0A>`, meaning a period (`.`), followed by a carriage return (`CR`) and a line feed (`LF`).

Overview

Every e-mail server on the Internet that wishes to receive e-mail coming from other (maybe unknown) hosts on the Net must do so by implementing SMTP (Simple Mail Transfer Protocol). In some cases when both parties in the mail delivery process know each other, they can even use a different protocol provided they both agree on it. For the Internet though, the de-facto protocol used is SMTP and it is this the most widely spread.

SMTP does not require the implementation of a security mechanism simply because many hosts are not known to the SMTP server receiving the e-mail and there is no way to distribute security credentials amongst mostly unknown hosts. What SMTP does is to receive e-mails for one or more of the users whose mail accounts the server hosts. In some cases, when the SMTP server receives an e-mail for a user whose account it does not host, it can try to deliver the e-mail to a third party, either because it is an adjacent domain or because it knows how a path to the destination. This is known as "relaying" and is mostly used inside trusted networks as relaying has been abused mostly by spammers and it is now highly discouraged for use in public networks.

When a foreign SMTP server wants to deliver an e-mail to a user in our domain, it establishes a connection to our server and after identifying itself, requests that mail delivery be allowed by specifying who the e-mail is coming from. After that, the foreign server can give a list of one or more addresses the mail has to be delivered to. This allows one same copy to be sent to various users possibly without duplication. Finally, the e-mail is transmitted from the foreign server and when done it can either request delivery of other messages or just close the connection.

The SWP-SMTP proxy works between the local server and the foreign server by trapping the commands and obtaining from them all the information it needs to submit the e-mail for analysis by SWAE. From the list of recipients, it not only determines the names of the accounts in SWAE but also pre-validates them by letting the real SMTP server (the local server) determine whether they are valid or not.

Once the foreign server sends the actual data of the e-mail, the proxy begins sending the e-mail to SWAE using each individual account of the recipients, so that the e-mail is analyzed in a personalized way. Once SWAE returns the tagged e-mail, the proxy delivers it to the corresponding recipient in the local SMTP server.

In the end, the messages are delivered and shown to users by any means the server provides on the user side just as any other e-mail, but with the important difference that is has first been scanned and tagged appropriately by SWAE.

The user will have the choice on the line of action to follow regarding e-mails tagged as spam, either by moving them to another folder, discarding them or any other action.

Installation

In this section you will find the instructions needed to install SWP-SMTP in some of the platforms for which the binary form is distributed. This manual is probably outdated (unless you are seeing it directly from our website) and it may be possible that the instructions for a particular version of an operating system are not shown. If this is your case, please go to our website and get the latest version of this manual.

How to get a copy of a binary distribution

In http://www.spamwarn.com, you will find a copy of the SWP-SMTP proxy program for your particular platform. You need to check the version of your operating system and the type of computer in which you are planning to install it because binaries are compiled individually for each operating system/equipment pair.

If your operating system version or equipment is not shown in the lists, probably the program is still not available for that platform. You can get in touch with us at the addresses on the website to coordinate the generation of a binary version for your configuration.

Steps for installation in FreeBSD 4.2

To install SWP-SMTP in FreeBSD, you will need administrative privileges in the system so you will need to be logged on as **root**.

Logged in as **root**, and having a compressed copy of the binary package, follow the next steps:

Uncompress the file with the following command, where ** is the version of SWP-SMTP that you got:

```
# gunzip swpsmtp-**_freebsd-4.2_i386.tar.gz
```

Now unpack the files contained in the `.tar` archive:

```
# tar -xvf swpsmtp-**_freebsd-4.2_i386.tar
```

Change the current directory to the directory where SWP-SMTP's files will be found:

```
# cd swpsmtp-**_freebsd-4.2_i386
```

Now copy the `swpsmtp` file to the `/usr/local/bin` directory

```
# cp swpsmtp /usr/local/bin
```

and the `swpsmtp.conf` file to the `/usr/local/etc` directory

```
# cp swpsmtp.conf /usr/local/etc
```

Finally, in order to have SWP-SMTP started each time the operating system starts, add the following line to the local startup file, `/etc/rc.local`. The same line is used from a command prompt to start the proxy.

```
/usr/local/bin/swpsmtp
```

This concludes the installation in FreeBSD. Before starting the proxy, it is recommended that you visit the Configuration section to learn which are the default options and what is their meaning.

You should also check your proxy configuration to avoid possible inconsistencies when there is a SMTP server already in use. For example, if the proxy is installed in the same computer where your e-mail server is running, you should ideally change the port where the server listens for connections to some other than port 25 (SMTP). This is because the proxy must listen in this port if the foreign servers are to connect to it. Otherwise, it will be necessary to configure the proxy and the possibly the firewall to communicate using a different port, and this is administratively much more costly.

Steps for installation in cygwin 1.14

The installation of SWP-SMTP in cygwin 1.14 on Windows requires that you are logged on as the system Administrator because it is mandatory that you first install cygwin 1.14 on the system.

As a first step, you must obtain and install cygwin 1.14. The cygwin installers, as well as the steps to do this can be found at the website http://www.cygwin.com. The rest of the steps for the installation of SWP-SMTP assume that cygwin 1.14 is installed in the default directory, that is, `C:\cygwin`. Also, make sure that you have the following packages installed for cygwin: `gunzip` & `tar`.

Having cygwin installed, follow these steps.

Start cygwin. To do this, from Windows you can go to Start->Run and type the following command line:

```
C:\cygwin\cygwin.bat
```

Once cygwin starts and the console appears, copy SWP-SMTP's installation file from the location where it was downloaded to, for example, C:\Downloads. ** is the version of SWP-SMTP that you downloaded.

```
$ cp /cygdrive/c/downloads/swpsmtp-**_cygwin-1.14_i386.tar.gz .
```

uncompress the archive with the following command:

```
$ gunzip swpsmtp-**_cygwin-1.14_i386.tar.gz
```

Now unpack the files within the `.tar` archive:

```
$ tar -xvf swpsmtp-**_cygwin-1.14_i386.tar
```

Change the current directory to the directory where SWP-SMTP's files are found.

```
$ cd swpsmtp-**_cygwin-1.14_i386
```

Now copy the `swpsmtp.exe` file to the `/usr/local/bin` directory

```
$ cp swpsmtp.exe /usr/local/bin
```

and the `swpsmtp.conf` file to the `/usr/local/etc` directory

```
$ cp swpsmtp.conf /usr/local/etc
```

finally, to have SWP-SMTP started each time the operating system starts, enter the `start.reg` file into the Windows registry by typing the following command:

```
$ regedit start.reg
```

and confirm the messages that appear.

This concludes the installation in cygwin over Windows. Before starting the proxy, it is recommended that you visit the Configuration section to learn which are the default options and what is their meaning.

You should also check your proxy configuration to avoid possible inconsistencies when there is a SMTP server already in use. For example, if the proxy is installed in the same computer where your e-mail server is running, you should ideally change the port where the server listens for connections to some other than port 25 (SMTP). This is because the proxy must listen in this port if the foreign servers are to connect to it. Otherwise, it will be necessary to configure the proxy and possibly the firewall to communicate using a different port, and this is administratively much more costly.

Configuration

In this section the configurable options of SWP-SMTP found in the `/usr/local/etc/swpsmtp.conf` file are presented. They are shown with the accompanying default values that the options take if not specified. To change these values just edit the file and restart the server.

Parameter	Default	Meaning
`MAXMSGSIZE`	`65536`	To avoid DoS or buffer overflow attacks, the maximum size that is allowed for messages. This is given in kilobytes. If no limit is desired, use a 0 (zero). The default value is 65536KB or 64MB. Although this may seem little to some, it is a pretty reasonable size, considering that almost no message will ever have that size. In any case, an attached file of 64MB or more should be sent by other means (e.g. FTP). NOTE: This value should be chosen carefully because the full message is stored in main memory while the program receives it.
`LISTENPORT`	`25`	As the name implies, the TCP port where the proxy will listen for connections. The default value is 25 which is the port number reserved by IANA for the SMTP protocol.
`SMTPSERVERIP`	`127.0.0.1`	The IP address of the real SMTP server which the proxy should connect to when required. The default value is `127.0.0.1`, meaning the localhost, that is it will connect internally to a program in the same host.

Parameter	Default	Meaning
SMTPSERVERPORT	25	The port in which the real server listens for connections. This value is configurable so that if the server and proxy both reside in the same host they can listen on different ports. The default value is 25. NOTE: With the three default values given, the proxy and SMTP server cannot run on the same host. This is done intentionally so that the required adjustments are made to the proxy, the SMTP server and/or the firewall.
SWAESERVERIP	127.0.0.1	The IP address of the SWAE server where the proxy will send the e-mails for analysis.
SWAESERVERPORT	7923	The TCP port where the SWAE server listens for connections.
SYSLOGLEVEL	NOTICE	The cumulative level that the system will use to define which events generate an entry in the log and which don't. Selecting a level includes all the levels above it. For example, SYSLOGLEVEL=CRITICAL implies that messages in the CRITICAL, ALERT and EMERGENCY categories will all generate an entry in the log. Available levels are: -EMERGENCY : Messages meaning that the system is unusable -ALERT : Messages that require immediate action -CRITICAL : Messages that describe a critical condition -ERROR : Messages that describe an error -WARNING : Messages representing an emergency -NOTICE : Messages informing of normal but important events -INFO : Purely informational messages -DEBUG : Messages used in the debugging of the system

Conclusions

The proxies accompanying the SWAE server program are extremely easy to use and do not require maintenance once they are installed.

The SMTP proxy becomes a great alternative for those environments in which the users connect to the server using protocols other that POP3 (e.g. Microsoft Exchange, Lotus Notes). It also has the advantage of being light and the possibility of sharing the host with the SWAE server, the SMTP server or both.