	Name: Description - SSH conversation injector		
№	**Number, version**	**Date**	**Author**
1	Version 1.0	12 July 2016	Konstantin Mauch, Senior Software Engineer

Preamble

Accessing CLI interface of SoHO hardware (produced by TP-Link) in some cases implies running SSH-based conversation with this hardware. To automate this conversation it's recommended to use 'SSH Conversation Injector' which is represented in given document.

Introduction

The 'SSH Conversation Injector' or 'convinject' for short, is a software framework (i.e. set of libraries, executables, and shell scripts) which emulates SSH commands (addressed to SoHO device) being issued by local host. It uses LIBSSH and OpenSSL development libraries and CLI vocabulary.

Being passed an exact set of CLI commands as input on program start it generates a set of SSH requests to post these command over SSH.

The framework 'convinject' was tested on TL-SL5428E ver2.3, and most of below operations have successfully passed the testing.

The framework 'convinject' is still under development and its up-to-date revision is permanently stored at https://github.com/metallistov20/convinject . Feel free to deploy under your tasks and to contribute.

The framework's prospective is: on achievement stable version to be merged with 'trafinject' project in scope of upgrading both projects with higher level navigating interface.

Functionality description

Present implementation of framework 'convinject' takes command line parameters: target host IP, username (-l parameter) and establishes the SSH session with host defined by target host IP with user defined username (-l parameter). The password for current SSH session – as well as in case of 'trafinject' project – is hardcoded, for the same reason as in case of 'trafinject' project.

Once SSH session is established, the framework 'convinject' inspects local folder for presence of 'local_data.txt' nad once found parses it line-by-line. Each line is regarded to be s single CLI command. Once found and correctly parsed it start to issue these command to target hardware – SMB switch produce by PT-Link.

	TP-LINK®	**Name:** Description - SSH conversation injector	
№	**Number, version**	**Date**	**Author**
1	Version 1.0	12 July 2016	Konstantin Mauch, Senior Software Engineer

Usage from within BASH shell

Here's a brief instance of what's going to happen if the user wants to deploy the framework 'convinject' in order to execute the sequence of following commands: <show port isolation>, <history>, <ping 192.168.1.1>, <tracert 192.168.1.1>, <ping 127.0.0.1>, <tracert 127.0.0.1>, <history>, <exit>, *consequently*.

Firstly user need to place these commands into 'local_data.txt' and to launch <./convinject 192.168.1.1 -l admin>, where <192.168.1.1> is and IP and <admin> is administrator's username of target SMB hardware. On launch the SSH session to target hardware is established and CLI session is being opened. As the first command to this session the <show port isolation> is executed. The output from this command is passed to STDOUT, so the user can observe the output strings. (Note: presently the output is being redirected to dedicated file, which is purposed for better flexibility of framework.) Next command to be executed and to give out the output is <history>, and so on. As the last command is <exit> the CLI session is closed, which hence does not mean the end of SSH session established with target SMB hardware. In order to stop that one the Ctrl+C sequence is required, which terminates the zsession and program at one time.

References

https://www.openssl.org/docs/faq.html

http://api.libssh.org/master/libssh_tutorial.html

http://www.tp-link.ua/resources/simulator/TL-SL5428E/Index.htm

https://www.youtube.com/watch?v=VQ0YvL2F7yU

https://en.wikipedia.org/wiki/Secure_Shell

https://github.com/metallistov20/convinject

№	Number, version	Date	Author
1	Version 1.0	12 July 2016	Konstantin Mauch, Senior Software Engineer

Table of contents