ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Information Security
www.infsec.ethz.ch

Semester thesis for Adrian Schüpbach

Firewall Testing with NAT

an extension to fwtest v0.6

Supervisor: Diana Senn
Professor: Prof. D. Basin
Issue Date: October 2005
Submission Date: February 2006

1 Introduction

We live in a world where all the company networks are connected to the Internet. Nobody can control the Internet, therefore a company has to protect their data from unauthorised access through the Internet. This is done by firewalls whose analogon in the physical world are locks. Everybody understands that doors need to be locked to prevent unauthorised access. It is the same in the digital world: unauthorised access to a companies network should be prevented, and this can be done by one or several firewalls.
Using the analogon of the door lock again, everybody understands that it is not enough to have a door lock. Only if the lock is locked properly and only authorised people have got a key to unlock it, we have what we want. It is the same in the digital world. It is not enough to have a firewall. We can only be satisfied if the firewall is doing what we expect from it. And to find out if a firewall satisfies our expectations (stated by a policy) we need to test it.

2 Motivation

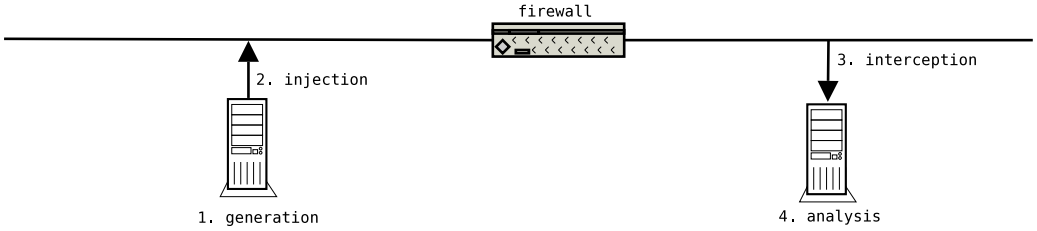

Figure 1: Flow of the Test Packets

Firewall Testing consists of two parts: the theoretical part of finding adequate test cases, and the practical part of running these test cases (each consisting of one or more test packets) on the real system. The aim of this thesis is to cover the second part.

Running test cases on a real system consists of four steps as shown in figure 1. The first step is the generation of the network packets. According to a given test case the corresponding network packets have to be built. The second step consists of injecting the packets generated in step one into the network. The third and the fourth step are then to intercept the packets which were injected in step two behind the firewall, comparing them to the expectations, and logging the result.

3 Assignement

3.1 Objectives

During his diploma thesis [1], Gerhard Zaugg has written a simple tool – named fwtest – which can do the above for TCP packets in a bidirectional way. This tool is a good starting point, but there are some things that need further work. Two of them should be looked at in this thesis: NAT and Timing.
As figure 1 shows there are two parties involved in testing which need some kind of synchronisation for being able to conduct bidirectional tests. For the first version of fwtest we decided to use time (and the NTP protocol) for this purpose. Unfortunately we had to find out in our tests at the end that this does not work very good. So one goal of this semester thesis is to combine these two parties into one, as shown in figure 2, and to find another way (than timing) of specifying test cases, i.e. which test packet belongs to which test case and in which order.
The second goal is to be able to handle NAT, i.e. to give the possibility to the tester (the person using fwtest) to specify every packet twice: how it looks before the firewall, and how he expects it behind the firewall. Also the tester should be able to use variables, which are then instantiated during testing. For example if we know that the firewall will translate every source IP and port to its own IP and some port. Then we just want to set a variable for this port in the specification of the test case to denote that there will be any number but that it has to be the same for the whole test case.

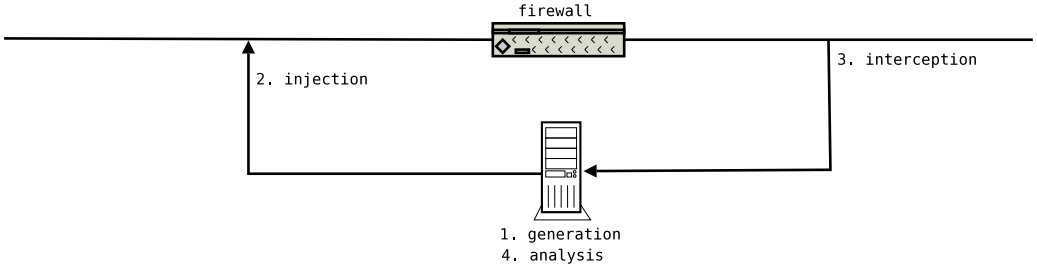

Figure 2: A single instance of fwtest

3.2 Tasks

- Understanding fwtest
- Designing a new generation of tp-file which knows test cases (instead of single test packets) and can cope with changing packets

- Adapting the parser to the new tp-file (no time, 2 versions of every packet, ...)
- Change the packet generation from preset (all packets are generated before testing) to adaptive (packets are generated when needed) to be able to take the newest information into account
- Changing fwtest to run as a single instance (instead of on two machines)

As there will be another student (Beat Strasser) working on fwtest in an overlapping time frame, some synchronisation between the two students is expected. This will mainly consist in determining a new format for the tp-files together and working on the same subversion repository.

3.3 Deliverables

- At the beginning of the semester thesis an agreement must be signed which allows the supervisor of this thesis, his project partners and ETH Zurich to use and distribute the software written during the thesis.
- At the end of the second week, a detailed time schedule of the semester thesis must be given and discussed with the supervisor.
- At the end of the diploma thesis a presentation of 20 minutes must be given during an Infsec group seminar. It should give an overview as well as the most important details of the work.
- The final report may be written in English or German. It must contain an abstract written in both English and German, this assignement and the schedule. It should include an introduction, an analysis of related work, and a complete documentation of all used software tools. Three copies of the final report must be delivered to the supervisor.
- Software and configuration scripts developed during the thesis must be delivered to the supervisor on a CD-ROM.

References

[1] Gerry Zaugg. Firewall testing. http://www.infsec.ethz.ch/people/dsenn/DA_GerryZaugg_05.pdf.

16th August 2005

Prof. D. Basin