Diploma thesis for Gerry Zaugg

Firewall Testing

Supervisor:	Diana Senn
Professor:	Prof. D. Basin
Issue Date:	27th September 2004
Submission Date:	26th January 2005

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

Firewall Testing consists of two parts: the theoretical part of finding adequate test cases, and the practical part of running these test cases 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

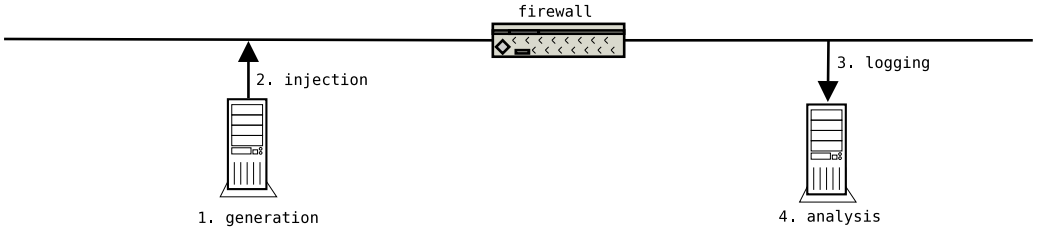

Figure 1: Flow of the Test Packets

the generation of the network packets. According to a given test case the corresponding network

packets have to be built. This can be done using existing tools [2, 1, 3]. An example of a test case could be:
(syn: A $->$ B)(syn & ack: B $->$ A)(ack: A $->$ B) (fin & ack: A $->$ B) (fin: A $->$ B)
for some source A, some destination B and some proto C. The second step consists of injecting the packets generated in step one into the network. In the case where we have only one firewall this is easy and can be done directly before the firewall. But in real world examples we normally have many firewalls. There it is much more challenging to find the correct place to inject a packet into the network. If we fail to do that correctly we risk some tests to fail because of that. The third step consists of logging the packets which were injected in step two. This log is then compared, in step four, with the injected packets of step two. As a test case consists of test data (from which the packets were generated) and an expectation, we now have to check for every packet if our expectations were fulfilled. If the outcome of a test is not as expected, either if a packet reached a place we did not expect or if a packet did not reach a place we expected it to, this should cause an alarm. This alarm is then analysed by a human person to find the source of the error. Therefore this analysis has not to be covered by this thesis.

3 Assignement

3.1 Objectives

The goal of this thesis is to design and implement a tool for the automated execution of tests according to given test cases as explained in Section 2. The tool should work on the 1-firewall-scenario. But it should be no problem to extend it to the n-firewall-scenario. Also there should be ideas on how to extend the solution to the n-firewall-scenario.

3.2 Tasks

- Searching of related work and tools.
- Evaluation of the tools found.
- Designing a solution for the 1-Firewall-Scenario.
- Implementation of the solution.
- Simulation and evaluation of the implementation.
- Evaluation of the n-Firewall-Scenario. Discussing the differences to the 1-Firewall-Scenarion. Sketching solutions.

3.3 Deliverables

- At the end of the second week, a detailed time schedule of the diploma thesis must be given and discussed with the supervisor.
- At half time of the diploma thesis, a short discussion of 15 minutes with the professor and the supervisor will take place. The student has to talk about the major aspects of the ongoing work. At this point, the student should already have a preliminary version of the written report, including a table of contents.

- 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 a summary 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] Salvatore Sanfilippo et al. hping. http://www.hping.org/.

[2] Jeff Nathan. Nemesis packet injection utility. http://www.packetfactory.net/projects/nemesis/.

[3] Mike Schiffman. The libnet packet construction library. http://www.packetfactory.net/libnet/.

27th September 2004

Prof. D. Basin