ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Information Security
www.infsec.ethz.ch

Semester thesis for Gabriel Müller

Timing, ... in Firewall Testing

Supervisor: Diana von Bidder
Professor: Prof. D. Basin
Issue Date: October 2006
Submission Date: February 2007

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.
Simplified, firewall testing consists of injecting packets before a firewall (at a node A), collecting packets behind the firewall (at a node B) and checking if ones's expectations for the firewall's behaviour were fulfilled. There exists a simple tool named fwtest [3, 2, 1] which implements this testing – in a bidirectional way – for TCP-, UDP- and ICMP-packets.

2 Motivation

Until now, sequence- and acknowledgementnumbers of and the time between two individual test packets were just set preset (= before testing). Also, test cases are executed serially. There are several problems with this approach:

- A firewall may act differently for different intervals between test packets.
- Pregenerated sequence- and acknowledgementnumbers are not correct in the case of lost packets.
- Parallel testing could drastically minimise testing time.

3 Assignement

3.1 Objectives

The idea of this semester thesis is to solve the problems given in Section 2. Namely, sequence- and acknowledgementnumbers should be set correctly just before sending a packet. The timing should be adapted to the environment, and independent test cases should be interleaved. For this different strategies shall be tried, their effects on firewalls shall be theoretically analysed and practically verified, and the best strategy shall be implemented.

3.2 Tasks

Timing:

- "Playing" with timing (using fwtest)
- Theoretical analysis of the timing problem
  - How to interpret different test outcomes due to different timing?
  - How to find the correct timing for testing?
  - ...
- Understanding fwtest
- Implementation of the chosen timing in fwtest[1]

Interleaving:

- Theoretical analysis of independence between test cases
- Algorithm for the Interleaving of test cases
- Implementation as shell script

Numbers:

- Changing fwtest as such that it uses correct sequence- and acknowledgementnumbers.

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 semester 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.

[1] It is important that information about the timing is written into the log-file. If time remains, a helper should be written to help users understand / interpret this information.

- 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] Adrian Schüpbach. Firewall testing with nat. http://www.infsec.ethz.ch/education/projects/archive/Bericht_Adrian.pdf, 2006.

[2] Beat Strasser. Extending fwtest to handle udp and icmp. http://www.infsec.ethz.ch/education/projects/archive/Bericht_Beat.pdf, 2006.

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

16th September 2006

Prof. D. Basin