Test Traffic Measurement Project

Security Document

Olaf Kolkman [*] *Henk Uijterwaal*[†]

RIPE NCC

March 27, 1998

Document: RIPE-179.ps
Version: 1.0

Contents

1 Introduction **1**

2 Securing the test-boxes **2**
2.1 The OS 2
2.2 Access 2
2.2.1 Physical access 3
2.2.2 Network access 3
2.3 System Monitoring 3
2.4 Additional comments 4

3 Measurement integrity **4**

A Procedure: Request for local support **5**

B Procedure: Emergency shutdown **5**

C Test Traffic Contact information **6**

1 Introduction

This document is part of a series that describes the design, setup and implementation of the Test-Traffic project at the RIPE-NCC. [1]. Here we will discuss

* Email: okolkman@ripe.net
† Email: henk@ripe.net

the security issues that are relevant to the test-traffic measurement program. This is a dynamic document, which will be updated when need arrises.

The test-traffic measurement boxes are connected to networks that are vital for ISP operations. Some of the security issues that come to mind when thinking about of hosting such a box are:

- Use of the test-boxes to generate a very high load on the network. (Denial of service attack).
- Using the test-box as a stepping stone to other machines in the network.
- Using the box as a packet sniffer. However, if a measurement machine should be compromised it will not be useful for packet sniffing if it is on a switched network. If there is the possibility to put the test-traffic machine in a switched network we advice to do so.

These kind of 'attacks' can only be done by persons having control over the test-measurement box. In the section 2 we describe how we secure the test-boxes so that only authorized personnel can access the machines.

Not important for the day-to-say operation of the hosting ISP but important to the project itself is the issue of data integrity. In section 3 we will address the issues that have to do with the measurements itself.

2 Securing the test-boxes

Our policy is to implement mechanisms and procedures so that only authorized personnel has access to the machine. To check the success of these measures we constantly monitor the system on unauthorized changes.

2.1 The OS

The operating system we the test-boxes is FreeBSD 2.2. Since this operating system is freely available, 'hackers' might find security holes faster than in proprietary systems. On the other hand there is a broad user base that checks and upgrades the system if needed. The open nature of the OS also implies that the security policy cannot be based on 'security through obscurity'.

We actively track the mailing list and web sites on FreeBSD security issues and immediately take action when security holes are discovered.

2.2 Access

The machine is accessible via the network and physically through the use of a console.

protocol	protocol	port number
tcp	ssh	22
udp	ntp	123
	syslog	514
	router	520

Table 1: Services listening to external traffic

2.2.1 Physical access

Physical access to the machine should be restricted to persons that are trusted by the network operator where the box is positioned. The network operator should realize that somebody with access to the machine and proper knowledge can become root without difficulty.

Technical contacts at the site should only connect a console to the test-box when asked by RIPE NCC personnel. (See appendix A for further information on how such a request will be made)

2.2.2 Network access

Only ssh connections are allowed to and from the machine

Access to a user shell on the machine over the network can only be established using ssh [2]. The authentication takes place over an encrypted channel using RSA based authentication.

In order to reduce the risk exploits of (yet unknown) bugs in network daemons all the services except those that are strictly necessary for operations have been disabled. The disabled services include all the daemons from the rsh suite, telnetd and ftpd. Services 'listening' to specific ports are specified in table 1

To reduce the risk that a compromised system is used as a stepping stone we removed most of the network client programs (telnet, ftp etc) and utilities such as compilers. Note, however, that these measures do not provide security as such; a powerful shell language like Perl needs to remain on the system for the measurement software, can be used for any network client or server task. We believe that the disabling of these services has a delaying and hopefully discouraging effect on trespassers.

2.3 System Monitoring

The system is monitored using scripts that

- Check on the file system content,
- Check on change of file permissions and ownership.
- Check general system health (availability of resources etc).

The data generated by these scripts is collected and checked at by the test-traffic operators on a regular basis.

2.4 Additional comments

If we notice that a machine has been compromised we will contact the local technical contact (see section A) and take appropriate actions. If a technical contact at the ISP has a strong suspicion of a hacking attempt originating from our test-box at his site, he may switch the system off (see appendix B). We prefer you contact our operation staff first before performing an emergency system stop, but always contact us after a security related event.

The hosting ISP's can increase security in the following ways.

- Place the measurement machine in a locked rack in an area with access control.
- Be careful not to add the host name or IP address of the test-box in local configuration files. (As a bad example, you might run scripts that use your zone file as an input for /etc/host.equiv).

Please notify us when you are applying (router) filters. This will allow us to perform more efficient trouble shooting.

3 Measurement integrity

Measurement may be influenced either per accident or my malicious intend. Although we consider this very improbable, we can think of the following issues:

- Modification of time on the test-boxes. This might be done through the use of the ntp daemon control program xntpdc. As a countermeasure we only accept control commands from xntpdc after proper authentication.
- Denial of service attacks on the test-box or the local network. In cases this becomes an issue countermeasures can be configuring in routers of the hosting ISP.
- Benchmark optimizing. Although we consider this kind of attack very improbable we implemented handles in the software design to somewhat disguise the measurement packets.

In general, the data will constantly monitor on internal consistency.

References

[1] H. Uijterwaal, O. Kolkman, "Internet Delay Measurements using Test-Traffic, Design Note", RIPE-158.

[2] T. Ylonen, *"The SSH (Secure Shell) Remote Login Protocol"*, See `http://www.cs.hut.fi/ssh/RFC` for the current work on the RFC. The Unix implementation available from `ftp://ftp.cs.hut.fi:/pub/ssh`

Document history

- December, 1997. Olaf Kolkman. First draft release version 0a.
- February 5, 1998. Olaf Kolkman. Second draft release version 0b.
- February 28, 1998. Olaf Kolkman. Public release, version 1.0.
- March 27, 1998. Henk Uijterwaal. Put in RIPE document store.

A Procedure: Request for local support

The test-measurement boxes do not need any support from the local technical contact during normal operations. In the rare events that local support is needed the RIPE NCC operators will contact the local technical contact with a request for local support.

You can expect requests for operations by letter, email, phone or fax. Please check the identity of the requester in one of the following ways.

- Some requests for operations will come with a reference to the test-traffic web-site (`http://www.ripe.net/test-traffic`). If you do not find information concerning the request than do not perform any action on the test-traffic box but send a mail to `ops-tt@ripe.net`
- If the request is received by e-mail please check the PGP signature.[1]
- If the request is done by surface-mail, fax or telephone please call the RIPE NCC for confirmation. Telephone numbers can be found on our web-page or in section C.

If you doubt the reliability of a request please contact the test-traffic operator.

B Procedure: Emergency shutdown

Halting the machine is a task that is preferably performed by the test-traffic operator. However there might be cases a system needs to be shutdown. In the case such a emergency shutdown is needed proceed as follows.

- connect a keyboard and monitor to the box.
- Give the 3 finger salute (ctrl-alt-del)
- Contact the Ripe NCC test-traffic operators.

A power-cycle will normally be sufficient to reboot the machine.

[1] `http://www.ripe.net/test-traffic/pgp-key.html`

C Test Traffic Contact information

Address:	RIPE NCC
	Test Traffic Measurement Project
	Singel 258
	1016 AB Amsterdam
	The Netherlands
Telephone:	+31 20 5354444
Fax:	+31 20 5354445
email:	ops-tt@ripe.net (for operational issues)
	tt-project@ripe.net (for other issues)
URL:	http://www.ripe.net/test-traffic
Project Members:	Henk Uijterwaal
	Olaf Kolkman
	Daniel Karrenberg
PGP Fingerprint	pub 1024/861884CD 1998/02/05
	RIPE NCC Test Traffic Project
	Key fingerprint =
	97 B5 07 E3 66 23 FA 35 9C 5B A3 07 00 6D B7 36