

Firewall Challenge report

January 7, 2009

Tested product: Jetico Personal Firewall 2.0.2.8.2327
Product vendor: Jetico, Inc.
Testing platform: Windows XP Service Pack 3
Number of tests: 84

Level reached: 10+
Total score: **89 %**

Introduction

This report presents results of *the Tested product* in the series of tests known as [Firewall Challenge](#). All the information regarding these tests, testing methodology and scoring system is available on [the website of this project](#). Reports of the commercial testing usually contain results of all available levels, reports of the public testing usually contain results of the first level and the following levels up to the highest level reached by the tested product. Public testing results are always published on the project's website, while the results of commercial testing are published only after the consent of the paying customer. The total score is always calculated as if the report was public.

Note that the number of levels, the number of tests or even the tests implementation may change. The report's results are valid at the day of the report's release and are not guaranteed to be valid after that day.

Testing results

Level 1

Level up: 50 %
Product's score: 100 %

Test name	Result	Comment
Breakout2	100 %	PASSED
Coat	100 %	PASSED
ECHOTest	100 %	PASSED
Kill1	100 %	PASSED
Kill2	100 %	PASSED
Leaktest	100 %	PASSED
Tooleaky	100 %	PASSED
Wallbreaker1	100 %	PASSED
Yalta	100 %	PASSED

Level 2

Level up: 50 %

Product's score: 78 %

Test name	Result	Comment
AWFT1	100 %	PASSED
DNSstest	100 %	PASSED
Ghost	100 %	PASSED
Jumper	0 %	FAILED – See the further notes at the end of the report.
Kill3	100 %	PASSED
Kill3b	100 %	PASSED
Kill6	100 %	PASSED
Wallbreaker3	100 %	PASSED
Wallbreaker4	0 %	FAILED – See the further notes at the end of the report.

Level 3

Level up: 50 %

Product's score: 100 %

Test name	Result	Comment
AWFT3	100 %	PASSED
AWFT4	100 %	PASSED
DNSstester	100 %	PASSED
Kernel1	100 %	PASSED
Kill3f	100 %	PASSED
Kill4	100 %	PASSED
Kill7	100 %	PASSED
SSS2	100 %	PASSED
Suspend1	100 %	PASSED
Thermite	100 %	PASSED

Level 4

Level up: 50 %

Product's score: 85 %

Test name	Result	Comment
CopyCat	100 %	PASSED
CPIL	100 %	PASSED
CPILSuite1	100 %	PASSED
Kernel1b	100 %	PASSED
Keylog1	0 %	FAILED
Kill3e	100 %	PASSED
Kill8	100 %	PASSED
Kill9	100 %	PASSED
SSS	50 %	FAILED – Unwanted user logout was not prevented.
Suspend2	100 %	PASSED

Level 5

Level up: 50 %

Product's score: 92 %

Test name	Result	Comment
Breakout1	100 %	PASSED
CPILSuite2	100 %	PASSED
Crash1	100 %	PASSED
Crash2	100 %	PASSED
Crash3	100 %	PASSED
Crash4	100 %	PASSED
Kernel2	100 %	PASSED
Kernel3	100 %	PASSED
Keylog2	0 %	FAILED
Kill3c	100 %	PASSED
Kill3d	100 %	PASSED
VBStest	100 %	PASSED

Level 6

Level up: **50 %**
 Product's score: **100 %**

Test name	Result	Comment
CPILSuite3	100 %	PASSED
Crash5	100 %	PASSED
Crash6	100 %	PASSED
DDEtest	100 %	PASSED
ECHOTest2	100 %	PASSED
FireHole	100 %	PASSED
Flank	100 %	PASSED
Kernel4	100 %	PASSED
Keylog3	100 %	PASSED
Keylog4	100 %	PASSED
Kill10	100 %	PASSED
Kill11	100 %	PASSED
Runner	100 %	PASSED

Level 7

Level up: **50 %**
 Product's score: **67 %**

Test name	Result	Comment
BITStest	100 %	PASSED
FireHole2	100 %	PASSED
Keylog5	0 %	FAILED
Keylog6	0 %	FAILED
Kill12	100 %	PASSED
OSfwbypass	100 %	PASSED
Runner2	0 %	FAILED
Schedtest	100 %	PASSED
SSS3	100 %	PASSED

Level 8

Level up: **50 %**

Product's score: **88 %**

Test name	Result	Comment
Kernel4b	100 %	PASSED
Kernel5	100 %	PASSED
Keylog7	100 %	PASSED
Kill5	100 %	PASSED
NewClass	100 %	PASSED
Schedtest2	0 %	FAILED – See the further notes at the end of the report.
SocketSnif	100 %	PASSED
SSS4	100 %	PASSED

Level 9

Level up: **50 %**

Product's score: **50 %**

Test name	Result	Comment
Crash7	0 %	FAILED
Driver Verifier	100 %	PASSED

Level 10

Level up: **100 %**

Product's score: **100 %**

Test name	Result	Comment
BSODhook	100 %	PASSED
ShadowHook	100 %	PASSED

Further notes

Regardless the indirect access to network alert, Jetico failed Jumper test because it did not block rewriting Internet Explorer's start page. If Jumper is terminated before the user starts Internet Explorer's process, the browser is redirected without any alert. Similarly, Jetico failed Wallbreaker4 and Schedtest2. If Wallbreaker4 and Schedtest2 are terminated just after new tasks are scheduled the browser is redirected to the target page.

Although Jetico passes many tests, it is sometimes unusable if an action of a malicious code is blocked. It happens with Jetico that the system must be rebooted to be usable again – e.g. to be able to surf the web. In case of a malware

Matousec – Transparent security

Firewall Challenge report



attack the usability of the system with Jetico might be quite low.