

Proactive Security Challenge report

October 29, 2009

Tested product: Norton Internet Security 2010 17.0.0.136
Product vendor: Symantec Corporation
Testing platform: Windows XP Service Pack 3
Number of tests: 84

Level reached: 8
Total score: **67 %**

Introduction

This report presents results of *the Tested product* in the series of tests known as [Proactive Security 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: 89 %

Test name	Result	Comment
AWFT1	100 %	PASSED
DNSstest	100 %	PASSED
Ghost	100 %	PASSED
Jumper	0 %	FAILED
Kill3	100 %	PASSED
Kill3b	100 %	PASSED
Kill6	100 %	PASSED
Wallbreaker3	100 %	PASSED
Wallbreaker4	100 %	PASSED

Level 3

Level up: 50 %

Product's score: 70 %

Test name	Result	Comment
AWFT3	100 %	PASSED
AWFT4	100 %	PASSED
DNSstester	100 %	PASSED
Kernel1	0 %	FAILED
Kill3f	0 %	FAILED
Kill4	100 %	PASSED
Kill7	100 %	PASSED
SSS2	0 %	FAILED
Suspend1	100 %	PASSED
Thermite	100 %	PASSED

Level 4Level up: **50 %**Product's score: **80 %**

Test name	Result	Comment
CopyCat	100 %	PASSED
CPIL	100 %	PASSED
CPILSuite1	100 %	PASSED
Kernel1b	0 %	FAILED
Keylog1	100 %	PASSED
Kill3e	100 %	PASSED
Kill8	100 %	PASSED
Kill9	100 %	PASSED
SSS	0 %	FAILED
Suspend2	100 %	PASSED

Level 5Level up: **50 %**Product's score: **83 %**

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

Level 6Level up: **50 %**Product's score: **62 %**

Test name	Result	Comment
CPILSuite3	100 %	PASSED
Crash5	100 %	PASSED
Crash6	0 %	FAILED
DDEtest	0 %	FAILED
ECHOTest2	0 %	FAILED
FireHole	100 %	PASSED
Flank	0 %	FAILED – See the further notes at the end of the report.
Kernel4	0 %	FAILED
Keylog3	100 %	PASSED
Keylog4	100 %	PASSED
Kill10	100 %	PASSED
Kill11	100 %	PASSED
Runner	100 %	PASSED

Level 7Level up: **50 %**Product's score: **50 %**

Test name	Result	Comment
BITStest	0 %	FAILED – See the further notes at the end of the report.
FireHole2	100 %	PASSED
Keylog5	100 %	PASSED
Keylog6	100 %	PASSED
Kill12	50 %	FAILED
OSfwbypass	0 %	FAILED – See the further notes at the end of the report.
Runner2	100 %	PASSED – See the further notes at the end of the report.
Schedtest	0 %	FAILED – See the further notes at the end of the report.
SSS3	0 %	FAILED

Level 8

Level up: 50 %

Product's score: 25 %

Test name	Result	Comment
Kernel4b	0 %	FAILED
Kernel5	0 %	FAILED
Keylog7	100 %	PASSED
Kill5	0 %	FAILED
NewClass	0 %	FAILED
Schedtest2	0 %	FAILED
SockSnif	100 %	PASSED
SSS4	0 %	FAILED

Level 9

Level up: 50 %

Product's score: **Not reached**

Level 10

Level up: 100 %

Product's score: **Not reached**

Further notes

Technically, NIS passed Runner2 because a popup query was displayed and the user had a chance to block the attack. However, the query asked about the original Internet Explorer accessing DNS server and the recommended action was Allow always. It could be assumed that common users would allow the action.

NIS failed Flank, BITStest, Osfwbypass and Schedtest because its protection relies on the specific implementation of these tests. NIS does not protect against the techniques of these tests. This was proved using slightly modified versions of these tests.