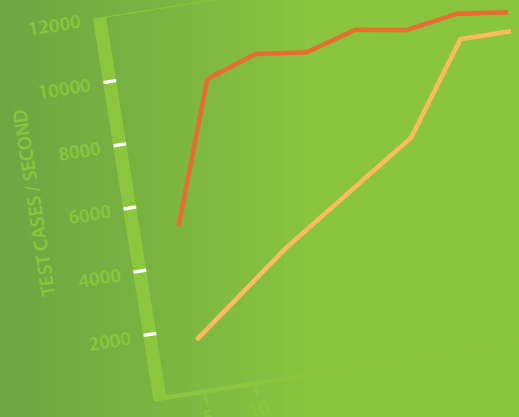


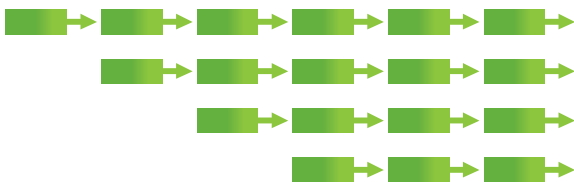
FUZZING PERFORMANCE



Increasingly complex technologies and faster product release cycles create a need for faster and more effective testing. Testers need to run more tests in much shorter time frames. To achieve this, testing platforms need to be able to run faster sequential tests and to run more test cases in parallel.

Defensics is a flexible and scalable fuzzing solution for security testing. It can generate and execute thousands of test cases per second. As a software-based solution, Defensics is not restricted by the hardware constraints of any specific testing appliance. Moreover, it allows test automation with the help of scripts.

At Codenomicon, we conducted a study to see how scalable the Defensics testing platform is. To reach fuzzing performance limits, we used a number hardware setups to test how many parallel Defensics suites can be executed simultaneously and how many test cases can be executed per second.



"One of the most important aspects of fuzzing is how fast you can execute test cases", says Dr. Charlie Miller, principal analyst from Independent Security Evaluators. "The faster you can execute test cases, the more test cases you can run and the more vulnerabilities you will find."

CODENOMICON Ltd.
info@codenomicon.com
www.codenomicon.com

Tutkijantie 4E
FIN-90590 OULU
FINLAND
+358 424 7431

10670 North Tantau Avenue
Cupertino, CA 95014
UNITED STATES
+1 408 252 4000

25/F, Queen's Road Centre
152 Queen's Road Central
HONG KONG
+852 3426 22900

Defensics for Performance

Defensics automates robustness testing and fuzzing. The platform can be used to generate test cases containing both valid and invalid traffic, thus it can be used for all types of functional protocol testing, namely:

1. Robustness and fuzz testing
2. Load and performance
3. Features

Defensics provides model-based test suites for over 200 protocols. All other protocols can be tested with the Codenomicon Traffic Capture Fuzzer, which can be used to replay and test any communication protocols captured by commercial and open source network analyzers. Defensics testing platform is used by hundreds of companies and organizations around the world for various purposes ranging from fast prototyping projects to more complex conformance testing solutions, which test complex specifications with hundreds of carefully built use cases.

Performance Metrics for Fuzz

To test how suitable the Defensics fuzzing platform is for high-speed robustness testing, we test how many test cases it can generate and execute per second. The load generated in performance tests is the result of two factors: the amount of sessions the test suite is running sequentially and in parallel.

The key metrics for fuzzing performance testing are:

- Amount of sequential test cases executed per second by a test suite
- Number of test suites running in parallel
- Amount of test cases executed per second by all parallel test



Features

Defensics features that impact test generation and execution performance:

- **Command-line execution:** Easy to reproduce complex test scenarios.
- **Multi-process execution:** On one host or distributed to multiple hosts.
- **Multi-threaded execution (select test suites):** Saves both the memory and CPU resources.
- **Looping a test case:** Reduces test generation overhead.
- **Looping all test cases:** Reveals performance degradation issues.

Benefits

- **Cost-effective:** Optimize hardware cost and reuse.
- **Best performance:** Supports for latest hardware platforms.
- **Test Coverage:** Systematic and thorough tests provide.
- **Protocol support:** Support for more than 200 protocols.
- **Turnkey solution:** Ready-made protocol models and test scenarios.
- **Tailorable tests:** User-editable protocol sequences and messages.
- **Rapid test creation and execution:** Test scenarios in matter of minutes.
- **Supports any IP protocol:** General purpose fuzzer for protocols.
- **Supports any file format:** General purpose fuzzer for file formats.
- **Concurrent test replication:** Load any test, and re-run the test
- **Automated test permutations:** Generate fuzz test cases from templates.

Test Results

HTTP and TLS protocols were chosen for the study. Running on 32-core system, the best average test case speed was 16,000 test cases per second for HTTP, and 2,400 for TLS. We did not observe significant difference in performance between multi-process and multi-threaded execution. In the figure, 5-threaded execution mode scales up faster as more test suites are started.

The theoretical test execution speed only depends on the number of CPUs available. Real test execution is approximately 40% slower than the theoretical speed due to the limitations of the operating system. Logging options also had impact, and with minimal logging the test speed increase was approximately 20%. Contact Codenomicon for assistance in selecting optimal hardware for high-performance fuzzing.