

### SYSTEM/DEVICE TESTING

# Mu-4000 Analyzer

REVIEWED BY ED SKOUDIS

**Mu Dynamics, Inc.**

[www.mudynamics.com](http://www.mudynamics.com)

Price: **Starts at \$40,000; \$300,000 with all modules—protocol mutations, published vulnerability and DoS—and gold support**



The Mu-4000 is a traffic generation, testing and test-monitoring tool focused on creating network attack patterns and illegitimate traffic, and measuring their impact on target machines. Since *Information Security's* last analysis of the Mu-4000 in December 2006, Mu has significantly increased the capabilities of its flagship product, adding new testing capabilities and monitoring options.

### Test Comprehensiveness **B+**

The Mu-4000 offers a vast number of different tests, including mutated traffic, published vulnerabilities and DoS attacks. The mutation engine is a top-notch commercial fuzzer, iterating through patterns of attack traffic, launching billions of different combinations of packets to find zero-day vulnerabilities in target software. Mu's published vulnerability analysis feature generates traffic for known attack vectors and flaws, including hundreds of buffer overflows and related problems.

The new DoS test suite allows testers to launch dozens of different DoS attacks, choosing from multiple protocols, including TCP, UDP and ICMP, with specialized payloads. When configuring DoS attacks, Mu supports ramp-up and ramp-down rates for traffic, letting an organization see if the target systems recover appropriately or are damaged or unstable.

**Testing methodology:** We configured the Mu-4000 to send a variety of packet mutations, published vulnerability attack vectors and denial-of-service attacks through a switch, router and network-based IPS device against a vulnerable target system running a variety of services, including Windows File and Printer Sharing, and a Web server.

### Security Testing Capabilities **A**

Mu offers one of the best fuzzing engines available and a comprehensive set of published vulnerabilities.

The system watches for service availability and response time during an attack, using a variety of instrumentation and monitoring options, including checking for system availability, service responsiveness, system log monitoring and more. When a fault is encountered, the Mu Analyzer supports stepping through groups of traffic and individual packets to determine which combinations of settings caused the problem.

### Setup and Configuration **B**

Given the increased types of tests and greater flexibility, creating a custom test involves numerous steps setting up the appropriate protocols, choosing from a myriad of options, and configuring the appropriate monitoring and instrumentation of the target device.

The GUI is organized to walk you through the various steps for configuration, but building custom tests is not for the faint of heart. To help, Mu has added the ability to create test templates, XML files that simplify creating and customizing an attack scenario.

All of the options for a given test can be saved as a template and exported from one Mu-4000 and imported into another. In addition, Mu ships dozens of pre-baked complex test templates in the product, with new templates released periodically.

The documentation is voluminous, but well written and illustrated, walking users through the complex setup and explaining the report format well.

### Reporting **A**

Mu's reports are easily understood, providing overall graphical representations of the test traffic generated, and the responsiveness of the target system under attack.

The Mu-4000 generates executive summary reports and assigns a letter grade based on faults and performance issues. Detailed metrics include not only service or system crashes, but also response time problems and the particular attack traffic that caused each problem.

### Verdict

The Mu-4000 offers comprehensive security testing, providing deep insight into how systems will fare under a barrage of attack traffic of all types. ▶