InfoWorld

InfoWorld 2008 Technology of the Year Award: Mu-4000 Security Analyzer

The Mu-4000 uses intelligent fuzzing logic to expose security weaknesses and performance issues in any device that talks to an IP network. Setup is a breeze, the GUI is excellent, and the Mu-4000 profiles security issues better than any other vulnerability assessment tool we've used. The Mu can even generate exploit binaries for newly discovered vulnerabilities. To top it off, Mu's intelligent workflow can turn untrained employees into a professional penetration team in a day.

Mu Security, Inc. is located at 686 W. Maude Avenue in Sunnyvale, CA. For more information go to www.musecurity.com or call Mu Security at 408-329-6330.

The Bottom Line

Mu-4000 Security Analyzer (Version 3.0)
Mu Security,
www.musecurity.com

Excellent 8.7

criteria	score	weight
Capability	9	30%
Ease-of-use	9	20%
Management	9	20%
Reporting	8	20%
Value	8	10%

Cost:
Ranges from $40,000 for eight protocols to $300,000 for a fully loaded system with 50+ protocols and subscription to one year of vulnerability signature updates

Platforms:
Linux-based appliance

Bottom Line:
The Mu-4000 uses intelligent fuzzing logic to expose security weaknesses and performance issues in any device that talks to a network. Intelligent, wizard-driven workflow makes tests a snap to configure, and the security profiles produced are top notch. The Mu can even generate exploit binaries for newly discovered vulnerabilities. A fully loaded appliance carries a hefty price tag, and a limited set of protocols is supported.

Mu Security Analyzer busts vulnerabilities with the greatest of ease

Mu-4000 fuzzer shines with wizard-driven test configuration, intelligent workflow, excellent vulnerability profiling, and auto-generated zero-day exploits

I first came across the Mu Security Analyzer when a coworker on a multicompany government project raved about how the appliance found a zero-day vulnerability in an e-mail inspection device that was protecting a top-secret government agency. It was a rather simple script bug in the other vendor's product, but it would have allowed uncontrolled code execution. The implication was that our top-secret project could have been compromised by an external hacker running penetration tests against our e-mail services. Initially, the manufacturer of the compromised mail filter refused to believe that a weakness existed in its product. That is, until we sent the exploit, automatically generated by the Mu analyzer, that the vendor's engineers could run to see for themselves.

Mu Security's Mu-4000 is a 2U appliance with RAID-configured drives and redundant power supplies that scans other computer devices using known vulnerabilities and malformed (fuzzed) traffic. The goal is to locate both security vulnerabilities and performance problems in the network. The Mu-4000 is constantly updated with the latest published vulnerabilities, but these types of exploits are not the Mu-4000's strong point. Published Vulnerability Attacks (or PVAs, as Mu Security calls them) only go back a maximum of three years and comprise slightly more than 1,000 exploits.

FUZZ BUSTER

The Mu's ability to intelligently fuzz traffic is its strongest selling point. Unlike vulnerability scanners or penetration tools that check only for known vulnerabilities, fuzzing can uncover previously unknown vulnerabilities by hitting network devices with mutations of normal packets and commands. The Mu-4000 understands more than 50 different protocols (IPv4, IPv6, VoIP, SIP, CIFS, ICMP, and SSH, among others) and can generate malformed traffic in millions of ways. The Mu-4000 includes the capability to automatically restart hung hosts and capture packet traces (in pcap form) of both sent and received traffic. The Mu can also capture what is going on in the target device's network interface or management port, and fire off scripts or kick-start other monitoring devices when a particular event happens.

I ran the Mu-4000 with its 3.0 release code in a test lab against several popular security appliances and a variety of different computer platforms. The Mu-4000 configures like most any security appliance. You plug a computer into its front console port, connect to the Mu's SSL management port, and configure basic IP information. After that, you can connect using an Internet browser, configure the rest of the device, and start your testing.

The Mu-4000 runs on a modified version of CentOS

(essentially Red Hat Linux), modified so that its IP stack will not choke on all the malformed traffic it will be sending. When the device is first started, you must install a license file that specifies which protocols may be attacked. Access to the Mu-4000 can be divided between system admins, who have complete control of the device, and regular users, who can see only results from scans that they create and run. The Mu-4000 has four IP interfaces that can be used in target analysis, and the device can create the attacks or be used as a pass-through device to record information you're gathering with another tool.

Because the Mu-4000 is easily capable of sending millions of attack packets, testing projects can get complex in a hurry. To simplify the process, Mu Security has smartly configured all scanning activity around analysis templates. Creating and using a template is essentially a step-by-step process that the Mu-4000 leads you through while it defines attack types, monitors, and actions to take in response to events. You select protocols and a myriad of custom attack parameters in an attack template. Monitors allow you to capture more information on the target, including from its own management console and log files. For example, if your attack locks up the target, the Mu appliance can capture what the target device's SSH-enabled management console looked like at the moment the device froze. Event triggers allow you to kick off external network monitors or initiate events such as file downloads on remote systems.

PEERLESS PROFILES

The resulting template is an XML file that can be sent to other Mu-4000 users so that they can duplicate your test. The management and configuration GUI is nearly flawless. It's helpful and wizard-driven to a fault. If you don't like GUIs, you can use XML files to drive the device instead.When the Mu-4000 finds a vulnerability, it will duplicate the attack to confirm that it is re-creatable and, if so, will then step itself through the entire attack sequence to find out exactly which string of sent information caused the fault. Network packet captures are standard, and that information is included with the information gathered by other monitors to profile the problem. The Mu-4000 profiles security issues better than any other vulnerability assessment tool I've used. Reporting itself is good, but not excellent. Detailed and summary reports are included, but the Mu doesn't allow easy customization of reports, nor does it hook into Crystal Reports, for example.

My testing found two previously undocumented security vulnerabilities and more than a few performance issues. In one case, a single malformed packet locked up the target so badly the firmware had to be re-imaged to regain control. One of the Mu-4000's best features is its capability to create a custom (Linux-based) binary that wraps any found vulnerability, essentially fingerprinting the security hole. You can download the self-documenting binary and send it to technicians so that they can re-create the problem without needing their own Mu-4000.

After running the Mu box, I asked myself why anyone should consider one of these pricey devices over the average free fuzzer off the Internet. First, the Mu-4000 has built-in fuzzing logic that you simply cannot find in free products. Mu's fuzzing is stateful, which allows the device to better mimic real-world conditions, and it is intelligent, methodically altering the state, structure, or semantics of a protocol in ways designed to expose weaknesses in the target. Mu's development staff understands how a problem in one area translates into high problem likelihood in another, and they have designed the tests accordingly. Also, the Mu-4000 contains business logic and workflow that can turn untrained employees into a professional penetration team in a day.

The Mu-4000 Security Analyzer gets my strong buy recommendation for any company worried about unknown security vulnerabilities, and for security device vendors trying to make their products as secure as they can be.

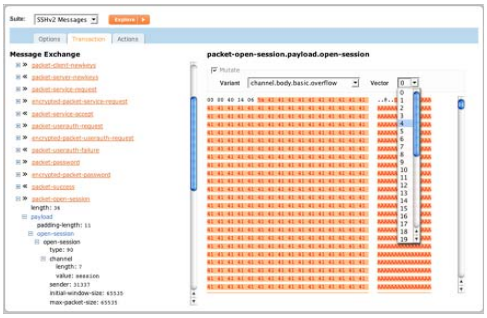
Roger A. Grimes is contributing editor of the InfoWorld Test Center. He also writes the Security Adviser blog and the Security Adviser column.

Mu-4000 Security Analyzer: A Guided Tour

Mu-4000 Security Analyzer

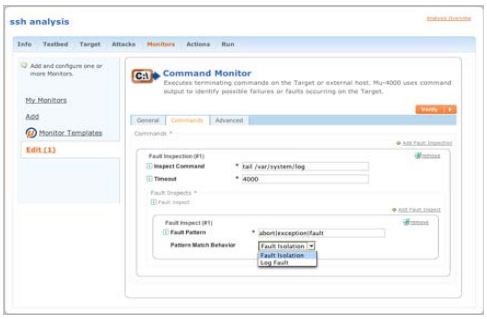
The Mu-4000 uses published vulnerabilities, existing external scripts, and a stateful fuzzer to find security weaknesses and performance limitations in network devices and applications. The Mu-4000 carefully monitors how the target device responds to protocol mutations -- dynamically generated packet streams designed to find software implementation flaws by violating the state, structure, or semantics of a given protocol specification.

Getting started
From the home page of the Mu-4000's Web-based UI, users can examine previously collected results, create new analyses, create and edit analysis templates, and configure and administer the appliance. A status window at the top of the page shows currently running processes, and lets you toggle among them.

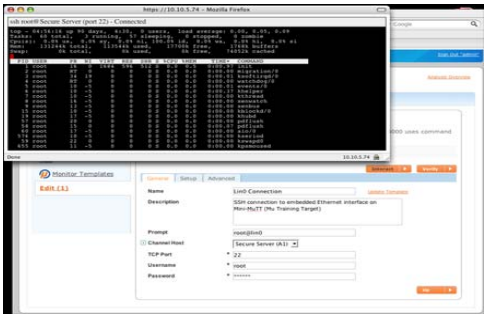


Setting up the test
After you set the IP addresses of the Mu-4000 interfaces and targets, configuring a protocol mutation attack starts with establishing a successful protocol-layer connection to the target. For example, in this view the multi-step exchange required to establish an SSH session is shown on the left, while the detail of a selected message is shown on the right. If you select a mutate-able message, you can then choose from a variety of mutation options and see how the mutation changes the packet.

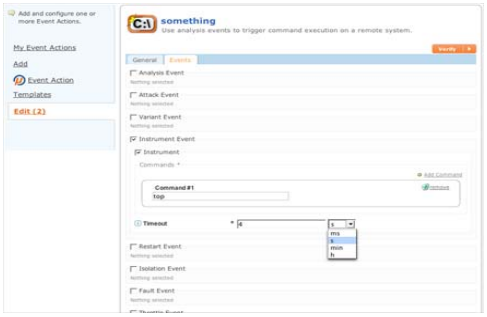
The more complex the protocol, the more difficult it is to find the right protocol configuration settings to create a successful connection. The mutation explorer helps point the way by listing the sequence of steps in the protocol exchange, highlighting exactly where failures occur, and decoding the protocol exchange down to the field level. The decodes show valid ranges for each field and the effect of the mutation on the formerly pristine packet.



Setting up monitors
Monitors allow users to observe what's happening inside the target device during a test. A monitor might use a serial console connection to the target, or an inline SSH or Telnet connection over the attack interface, or a separate system connected to the target by other means. A fault inspector, shown, is a command monitor that observes the output of a process, a script, or any other command run inside the target or a proxy monitor machine. Fault isolation is triggered based on pre-defined "interesting" output.

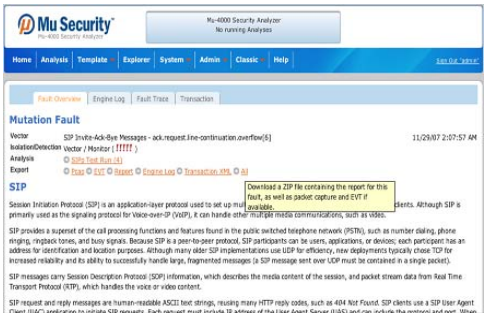


Target CLI
When setting up a monitor for a target that has a command line interface, it's useful to log in to the target manually and run some commands, check the output of a program, or examine the format of a log file. The Mu-4000 creates an interactive CLI inside the browser that is functionally equivalent to running a terminal emulation session from a laptop. Here we see the output resulting from typing the "top" command in the target-CLI window.

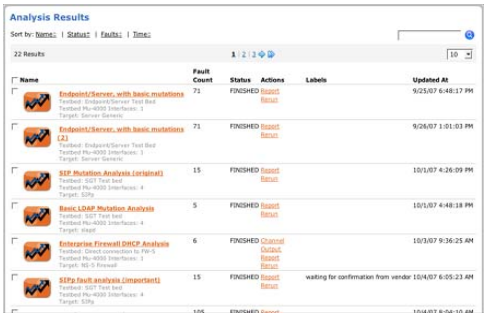


Event triggers
The Mu-4000 can execute a series of events at almost any stage of a lights-out analysis process. For example, if a fault is found in a long-running analysis, the Mu-4000 could log into a nearby system and run a script to send an SMS message to your cell phone. Here, the Mu-4000 is configured to record the output of the "top" command whenever it performs the valid test case, so as to track the activities of the top processes during the analysis.

Running the analysis
The next step is to run the analysis. As the Mu-4000 generates its test cases, an engine log monitors the progress in real time. After the analysis completes, users can look back at the recorded response-time or latency data (including the minimum, mean, median, and maximum values for each variant), as well as any fault conditions, collected for each protocol attack that comprised the analysis.



Investigating faults
The fault viewer provides detailed information on how the protocol works and how the Mu-4000 performed the testing. It also allows you to see the metadata associated with each fault, including a packet capture, a proof-of-concept exploit in the form of a Linux executable, a manager-friendly report, the engine log showing the fault isolation procedure, and an XML file detailing the protocol exchange.



Repeatable results
All aspects of an analysis configuration can be saved as editable and shareable XML templates. These templates are easy to re-run to show repeatable results (as shown by the first two analyses here) or to verify a fix. After a patch or update is made available, simply locate the original analysis and click the "Rerun" link.