

NSS Labs tests 13 leading intrusion prevention systems

Date: Fri, 03/04/2011 - 13:56

Five vendors achieve recommend rating, but wide ranges in effectiveness, performance and value prove that buyers should carefully review products before purchasing



Rick Moy, president, NSS Labs, at NetEvents EMEA Press Summit, Barcelona

NSS Labs, Inc., the leading independent security testing organization, recently announced the release of its latest Network Intrusion Prevention System (IPS) Comparative Group Test Report for the fourth quarter of 2010.

Key findings from the report show:

- Security effectiveness has improved on average since 2009 to 62% (default). With some default policies as low as 31%, tuning remains crucial for most solutions. Several vendors still failed the anti-evasion testing, leaving gaping holes in defenses.
- Performance has decreased in general over the last year, with one vendor achieving just 3% of its claimed throughput.

- For the first time, a few multifunction gateways are proving a credible alternative to stand-alone IPS products for mid-market deployments.

In the year since NSS Labs' last IPS test, attackers have refined their strategy and have increased both the volume and the intelligence of their attacks. "Drive-by" downloads and exploits have been combined with disciplined attacks such as Operation Aurora, and the Zeus and Skynet botnets which target financial institutions. These test results point towards the need for organizations to continually evaluate their IPS options to make sure they are not overpaying for an underperforming solution.

NSS Labs compared the products head-to-head against 1,179 live, enterprise-class exploits using its real-world testing methodology. Products were tested using the vendor's default or "recommended" settings and then again as tuned by a vendor representative. New in this year's report is the Security Value Matrix (SVM), which allows enterprises to compare the cost and effectiveness of tested products on an apples-to-apples basis.

"Cyber criminals have all the time in the world to plan and attempt attacks. Our data and analysis are based on multiple man-years of complex, real-world testing that mimic how cyber-criminals are working to penetrate corporate defenses," said Rick Moy, president, NSS Labs. "This report answers the critical questions on product capabilities and limitations that enterprises cannot answer without great effort and investment in time, equipment, and specialized expertise."

<http://www.telecomkh.com/en/internet/products-and-services/intrusion-prevention-systems/netevents-emea-press-summit-barcelona-2011/nss-labs/2865>