

NASA Provides a Model for Effective Practice

The National Aeronautics and Space Administration has demonstrated the efficacy of a broad-based, targeted vulnerability scanning and remediation program -- for more than 80,000 computers in ten major facilities.

In the summer of 1999, the NASA CIO identified approximately 50 of the most serious vulnerabilities whose presence on a computer could be verified by network scanning tools. The CIO purchased and deployed to all Centers a standard suite of network scanning tools, and trained field security staff how to use them. The CIO required that all organizations report the scanning results to the CIO quarterly

Starting in Fiscal Year 2000, each quarter all network-connected NASA computers were scanned for the listed vulnerabilities, and system owners were informed of their vulnerabilities and how to eliminate them. Scanning data was transmitted quarterly to the CIO. The CIO set a target that each Center would achieve a ratio of fewer than one listed vulnerability per four computers scanned (or 0.25 vulnerabilities per system scanned.) Initially the observed ratio exceeded one, but by the end of FY00 it had dropped to 0.16, with over 80,000 systems scanned. For FY01 the target ratio was reduced to 0.01, and by the end of FY01 the ratio stood at 0.0068. An updated list of serious vulnerabilities was introduced in FY01 to replace the first list, with an initial target ratio of 0.25, and by the end of FY01 the ratio for that list stood at 0.097.

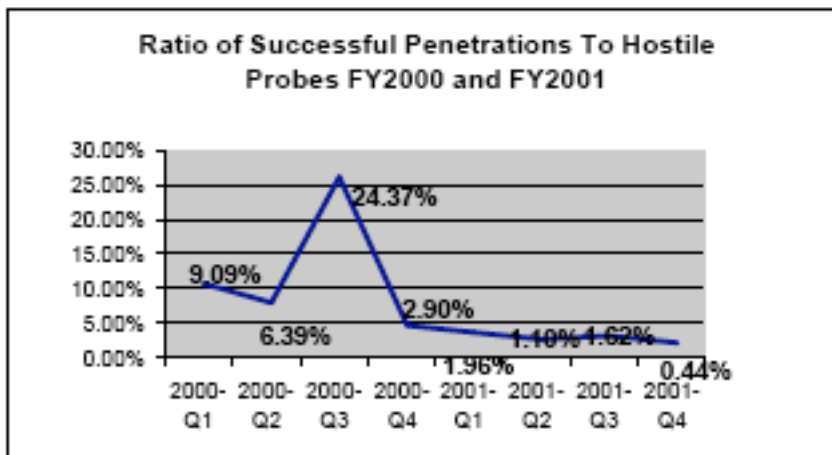
Healthy competition developed among Centers to reduce the ratio, and computer owners became more aware of and more involved with fixing vulnerabilities on their systems. For FY02, NASA further refined the process by updating the list each quarter to catch emergent serious vulnerabilities, keeping the same target ratio of 0.25. In addition, NASA has required emergency scanning, remediation and reporting for a few very fast-developing exploits.

The cost of this project is almost entirely in labor. Each of the ten NASA Centers devotes a substantial part of one or two staff (depending on Center size) to scanning, reporting, and monitoring, and individual system administrators assist them. Total cost is therefore between \$2 million and \$3 million per year, or about \$30 per computer per year.

NASA focused on the most important vulnerabilities, rather than all possible vulnerabilities, because NASA data, like that of other organizations, showed that a few vulnerabilities were responsible for most of our compromises. This made the problem of reducing vulnerabilities more manageable, and NASA security staff became skilled at using scanning tools. Because the agency standardized on the scanning tools and the vulnerabilities to be scanned, results were comparable among Centers. System owners became more aware of system vulnerabilities and the importance of fixing them. Quarterly metrics showed where they were making progress and let the CIO focus on weak areas. Regular practice in scanning for and fixing vulnerabilities made NASA more adept at dealing with fast developing exploits.

The number of system compromises has been reduced, even though attacks have increased markedly. Focusing attention on the most important vulnerabilities has kept the cost of fixing vulnerabilities lower compared with trying to fix all vulnerabilities, and has helped to maintain user support for the security program.

The figure above shows the ratio of successful penetrations to hostile probes, which are attempted attacks. At the first quarter of FY00, this ratio stood at 0.09, and after a very bad third quarter of FY00, it has continued to drop. At the end of FY01 the ratio stood at 0.004, or almost three times better than when NASA began its vulnerability reduction program. As a result NASA has been spared the cost of cleaning up additional compromises and consequences of disrupted services.



In addition, NASA appears to have fewer problems with fast-spreading exploits than they used to, because through the scanning program they have often eliminated the vulnerability before the exploit spreads. Because they are set up to rapidly scan for vulnerabilities and fix them, at the first sign of an emergency exploit warning, they can quickly identify and fix the vulnerability.

Of course, NASA has also improved other parts of its information security program, including better training, better attention to security plans, better security architecture, and better intrusion detection, so it is hard to attribute all of the improvement to vulnerability reduction. Nonetheless, the Agency believes targeted vulnerability scanning and elimination has been an important contributor to the improvement.

If you have any questions concerning this report please email me at paller@sans.org.