



Total Visibility

Network-mapping system helps government users comply with FISMA and improve their scores

BY ASHLEY ROE

A network security company is helping users to map and identify assets on their networks in a way that is analogous to how sonar enables oceanographers to map and navigate the unknown abyss we call the ocean.

IPsonar, the flagship product of Lumeta Corp., Somerset, N.J., provides users with total visibility of their network by mapping and identifying assets on the network, including the ones not currently under management. Unmanaged assets, according to the company, can increase the risk of network intrusion attempts and service outages. The tool thereby helps users analyze connectivity between their assets and the network and uncover risk patterns, vulnerabilities and policy weaknesses, thus bolstering their security procedures and improving their FISMA scores.

"With large, complex and dynamic networks, the pace of change is very high," says Michael Markulec, executive vice president of technology and operations for Lumeta. "With these changes, network defenses become misaligned with security policies over time, and agencies don't often realize this. They haven't necessarily looked at the network as a whole."

The system evaluates a user's network through four action modules: network

topology, host discovery, leak discovery and device fingerprint discovery. Network discovery traces the path of data on a network to indicate if assets are communicating properly and flags those assets that do not respond, signaling an unmanaged resource. Host discovery identifies the perimeter of a network by conducting a census of all visible IP addresses and noting previously unknown addresses. Leak discovery identifies devices with unauthorized inbound or outbound connectivity to the Internet or other sub-networks, and device fingerprint discovery detects active services and applications, improperly secured wireless access points and formulates a list of all devices running on network-based services. Users are provided with a series of analytical maps that catalog the data reported by each module. The end result, according to Markulec, is global network visibility.

"IPsonar provides a visual map of connectivity on the network using multi-protocol discovery so that IT executives have an accurate picture of what's connected - both managed and unmanaged," Markulec says. "With this

information, they can optimize vulnerability management, enhance network monitoring and change management processes to ensure that defenses are aligned with policy."

The technology was born out of the Internet Mapping Project, conceived by Bell Labs scientists in 1998, which aimed to determine the perimeter of the entire Internet through creation of a map of the routers present in North America. In 2000, Lumeta spun out of Bell Labs and adapted the project to suit the networks of corporations and government agencies. According to Markulec, 60 percent of IPsonar users are government agencies, and many of those agencies are using the system to aid in Federal Information Security Management Act, or FISMA, compliance.

In April 2007, the House Government Oversight and Reform Committee released FISMA scores for 2006. The grades are determined by annual reports that agencies prepare in order to comply with FISMA. The agencies are rated in various areas such as their annual tests of information security, their plans of action and corrective action plans, whether they certify and accredit their systems as secure, how well they manage the configuration of their computers to ensure security and their information security training programs.

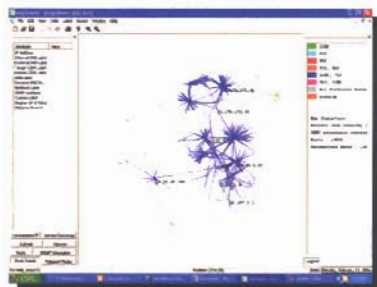
According to the results, nine government agencies earned lower scores than they did in 2005. Four agencies - the Departments of Commerce, Education, Treasury and the Nuclear Regulatory Commission - received Fs, and the federal government was granted an overall score of C-minus.

According to Lumeta, implementing E-Gov and IPv6 initiatives can elicit changes in network connectivity and the data flow among network assets, thus exposing security holes. This may cause government agencies to inadvertently lower their FISMA scores.

Tony Bilby, director of product solutions for Knight Point Systems, Herndon, Va., a government reseller of IPsonar, has three government clients using the system. "The bulk of government agencies use a host of

tools to provide different network security services, but they have not deployed an overarching tool," he says, adding that a lack of broader visibility might be a contributing factor to a lower FISMA score.

Adds Markulec, by using the system, agencies take a proactive approach in addressing network security issues and can increase their FISMA scores. ★



IPsonar provides a visual map of connectivity across a network. The information can be used to bolster logical security policies.