This month's group of products enable testing of the infrastructure, and make security assessments easy or, at least, easier, says Peter Stephenson.

The environments in which we all work have become more complicated as the years have passed, and one of the outcomes is that they are far more difficult to test for vulnerabilities. Today, we actively invite strangers into our networks. Well, not exactly all the way in,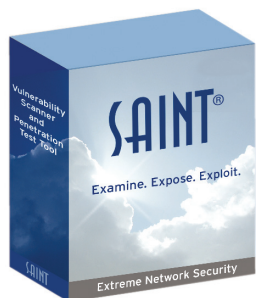 but far enough to cause concern if the perimeter is not very secure. Never before has the notion of layered security been more important.

Recently, I performed some testing on a web application. I knew the application had some holes, but my main concern was whether the holes could be reached from an attacker's location, wherever that might be. To do that, I needed to test vulnerabilities in the infrastructure.

These tools enable testing of the infrastructure. If applications are exposed to the outside, simple vulnerabilities become potential disasters. That means that the platforms they sit on and the routes to those platforms must be protected.

Scanner + Exploit

Vendor	SAINT
Price	$2,695, for a Class C network
Contact	www.saintcorporation.com

SAINT Scanner and SAINT Exploit 6.7.11 are two great tools wrapped up to work together to provide an in-depth view of vulnerabilities throughout a network. To be sure of total security risk, the integration of these products allows for not only vulnerability assessment, but also the attempt at exploiting those vulnerabilities.

While the SAINT Scanner uncovers the vulnerabilities, it is SAINT Exploit that is the true star of this combination. Exploit can run various exploits remotely, locally and through an already compromised target onto others throughout the network.

We found this product to be quite easy to use. Installation is done on a Linux platform, but we found we did not have to be Linux experts to run it. The installation steps really were the only command-based piece of this product, and the documentation outlined these step quite well.

Once installed, all of the administration is done through an intuitive GUI, with simple tab top navigation. We also found that these products were very well integrated with each other in the same interface, so there was no bouncing back and forth between them.

This product performed nicely in our test environment. After scanning was complete, we found that creating reports was quick and easy with SAINTwriter. These reports gave an excellent amount of detail in a nice easy to read format. It is also possible to view results quickly in the GUI itself, and all the results can be organized by severity, name or host.

Documentation comes in the form of a single PDF document. This guide includes all the necessary installation requirements and tasks, as well as a great amount of detail on configuring and using the product. We found this documentation to be well organized. However, we would have liked screen shots for easier understanding.

SAINT includes eight hours a day/five days a week phone and email technical support, while 24/7 support can be purchased for 10 percent of the list price.

At just under $2,700, this solution is a good alternative, or addition to, an already existing penetration tool for almost any size environment. It combines an easy-to-use look and feel with some highly comprehensive testing ability.

Vulnerability/penetration testing in one easy-to-use product.

— Peter Stephenson

SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★☆
Support	★★★★★
Value for money	★★★★★
OVERALL RATING	★★★★★

Strengths Vulnerability/penetration testing in one easy-to-use product.
Weaknesses Available only for Linux or Mac architectures.
Verdict We were really pleased to see how well this workhorse has matured over the years. It came within a hair of being our Recommended product.

SAINT®

SAINT Corporation
www.saintcorporation.com
1-800-596-2006 x0119 or
sales@saintcorporation.com