

STANDARD OPTIONS: FUZZERS & SPLOITS



CAN'T I DO THIS WITH FREE TOOLS? Yes and no. True, the new power-testing category is a synthesis of some great ideas pioneered within the freeware community for years. But, don't underestimate the massive amount of work needed to integrate these components into a functional testing suite.

For example, when *Information Security* tested network-based IPS tools ("On the Line," November 2005), we utilized a variety of these free tools. However, building our lab and integrating the components took months of effort. Coordination of traffic senders and impact on target systems required significant manual intervention and analysis. Instead, by buying a security testing tool rather than building your own from scratch, you are purchasing the integration of functional components in a coherent, professional-grade testing tool, minimizing the amount of custom scripting and manual analysis required.

Nonetheless, free tools are valuable resources. Among the most popular are the following:

Database of Known Exploits: The Nessus vulnerability scanner can measure for thousands of known flaws, and the Metasploit framework includes exploit code for more than 100 different vulnerabilities.

Transformation Engines: Fragrouter and Fragroute, by Dug Song, can fragment and perform various TCP tricks against packets in more than 30 ways to avoid detection. The Metasploit project includes several encoding engines to trick IDS and IPS tools.

Protocol Fuzzers: There are dozens of free fuzzers. SPIKE, a toolkit by Immunity, allows C developers to create protocol-fuzzing tools. The general-purpose fuzzers take packet-capture streams, analyze them to understand the protocols they contain and let users fuzz across different aspects of those protocols. File fuzzers, which generate files with various combinations of unusual fields in the file format, include FileFuzz for Windows and SPIKEfile for Linux.

Legit Traffic Load Generator: The popular tcpdump sniffer captures legitimate traffic and stores it in a packet-capture file. Stored legitimate traffic can then be replayed on a network using the tpreplay tool.

Traffic Editors: Nemesis and Hping2 create network traffic with specialized header field settings and payloads. NetDude is a graphical packet editor for Linux that allows users to alter various settings in the packets of a capture file. NetSED lets a user alter traffic streams passing through a system in real time.

Traffic Receivers: Sniffers are typically used to receive traffic, with the free tcpdump and Ethereal/Wireshark being the most popular.

Passive Monitors: Various free, open-source implementations of snmpd and syslogd tools can be used.

Active Monitors: These are usually implemented with custom scripts that log in to a target machine, run various commands and scrape the output looking for the status of given processes.

Reset/Reboot: Custom active monitor scripts sometimes include logic to restart processes or reboot machines when they are impaired.

Monitoring and analysis: This most important aspect of the analysis is often done using custom scripts and painstaking manual inspection. •