

Michael Fogel, Technical Business Unit Manager, State & Local Government, UNIFIED Technologies

Michael Jones, Systems Engineering Manager, UNIFIED Technologies

Security systems should be tested with network and hacker tools. Tests should represent both inside and outside attacks. External attacks may use tools such as SATAN, COPS and CRACK. Inside attacks can take place through modems, infiltration, social engineering, or by authorized users.

Networks should be tested using tools such as SATAN, COPS and CRACK. SATAN (System Administrator's Tool for Analyzing Networks) uses PERL scripts to gather network information. Even a light scan can identify network hardware and operating systems, client and server types, and so forth. Hackers use this information to research known vulnerabilities or to find holes in the configuration. COPS (Computer Oracle and Password System) examines individual computers to discover file directory device permissions, poor passwords, and other security holes. CRACK uses a digital dictionary to break passwords.

A complete security analysis involves defining an organization's current policy, performing an internal audit, performing external testing and generating reports. External testing includes using SATAN and other tools, as well as testing against known vulnerabilities. Case studies demonstrate a wide range of vulnerability between organizations. Some have few security holes; others fail to comply to their own security policy and have numerous holes.

One currently unresolved security issue is firewall certification. A third party such as CERT or NCSC could set up standards; or firewall vendors could create their own. Standards might include testing against known vulnerabilities, testing with SATAN and other tools, and reviewing firewall/network configuration. An organization would recertify every time its configuration changes. Planned periodic certification would ensure that the firewall meets new threats.

Beyond direct network attacks (addressed by firewalls), attacks may come through modems, through physical infiltration, through social engineering or by authorized users. Social engineering and attacks by authorized users are by far the most common threats. These threats can be addressed by interior firewalls as well as personnel policies and procedures. Note that a true security solution is just part of the network infrastructure. The solution must facilitate use or people will work around it.