SearchSecurity.com
Security School

Top tools for testing your online security

By Michael Cobb

Keeping a Web site secure is not just a case of relying on a firewall or hoping that a few short-term fixes will stop a problem from re-emerging. It is a continuous undertaking. By following a structured approach, you can make your security management tasks easier and increase your chances of success.

Security lifecycle

The initial hardening and configuration of your server is based solely on facts known at the time of set up. Reassessing a system on a continuous basis ensures that its security adapts and evolves to keep up with changes in technology that can affect the system and reduce the effectiveness of future attacks.

Lifecycle methodology

A lifecycle management process uses a standardized, repeatable set of procedures to upgrade, reassess and defend a site. Standardization ensures proper control over configurations of software and that tasks are executed in an orderly and predictable manner. Standardization also ensures no tasks are forgotten or left uncompleted. With well-defined policy guidelines an organization also ensures that responses to problems are suitably covered.

Lifecycle management means taking a long-term view and implementing proactive as well as reactive policies. For example, periodic vulnerability assessments ensure that you remain secure (proactive) and assess whether your policies support quick incident response (reactive). Always make sure those responsible for security have the training and the time to do the job. There is no point having regularly scheduled log reviews performed by someone who does not have the time or knowledge to analyze them effectively.

Assessing vulnerabilities

Vulnerability assessments are a critical process in the security lifecycle. They determine the security bill of health for your system. They should be planned as a regular part of your security maintenance procedures because vulnerabilities are continuously being discovered. You can use the same or similar tools to those of hackers to ensure your site is secure from attacks employed in the wild. My recommendations for free tools are:

- ❑ Network Mapper (Nmap) from www.insecure.org/nmap
- ❑ Nessus from www.nessus.org
- ❑ Microsoft Security Baseline Analyzer available from www.microsoft.com/technet/security/tools/mbsahome.mspx

Another option is to employ a Red Team to attack your system and uncover system weaknesses. This ethical hacking is a controlled simulation of an attack. Any holes found by the Red Team are fixed before a real intrusion occurs. Simulated attacks also provide your security team with realistic training in attack response.

Responding to an intrusion

Despite your best efforts, your server may be successfully attacked. First, consult your security policy, which should outline procedures for responding to the compromise. If you do not have a security policy, immediately consult with management to ensure the recovery effort is coordinated with other departments such as the media and legal teams.

Next, regain control of your system. Disconnect all compromised machines from the network, including any dial-in connections to prevent the intruder from defeating your attempts to recover the machines. After that, you may wish to operate in single-user mode in Unix or as the local administrator in Windows, to ensure that you have complete control of the machine. This will prevent users, intruders and intruder processes from accessing or changing state on the compromised machine while you continue the recovery process. Note, however, that if you reboot you may lose some useful information, because all processes executing at the time of discovery will be killed. Therefore, you may want to determine if the compromised system is running a network sniffer in order to remove it before rebooting.

If you are dealing with a mission-critical application, you probably cannot wait for the outcome of a detailed post-mortem to determine how the compromise occurred, so create a backup of your system. This will provide a "snapshot" of the file system at the time that the compromise was first discovered. You can refer to this backup in the future when analyzing the intrusion. You may also wish to contact law enforcement agencies to investigate the case.

To recover from the intrusion you must install a clean version of the OS and ensure all unnecessary services are disabled. Next, consult CERT advisories, summaries and vendor bulletins for the latest configuration guidelines for your OS, the services you are running and any security tools being used. Ensure that you install all vendor security patches and that all passwords are changed. Enable maximum logging for a while in case you are subject to another attack. Before you restore data from backups ensure that they have not been compromised by the attack.

Finally, as your Web site has been compromised, you must obviously look to enhance the security of your system and network before reconnecting it to the Internet. You will need to update your security policy to document the lessons learned and incorporate the changes made to the system. You should also calculate the cost of the incident to help with future risk analysis cost return calculations.

An excellent checklist and steps to follow to recover from a Unix or Windows system compromise is available at http://www.cert.org/tech_tips/root_compromise.html.

Top tools for testing your site's security and defenses

The following tools help analyze a security status in more detail and find indications of a system compromise.

Security scanners

You can't rely solely on patches to keep your system secure, but a good security scanner will help you find the holes that hackers exploit. The scanner typically launches probes, collects results and compares the results with a database of vulnerability fingerprints. In this sense, a security scanner is similar to a virus scanner but more introspective, determining whether devices comply with established security policy. Good vulnerability scanners provide documentation about the nature of any vulnerability found and links to further information and fixes as well as regularly-updated vulnerability checklists. In addition to commercial scanners, there are public-domain vulnerability scanners, such as ShieldsUP! (www.grc.com) and nmapNT (www.eeye.com).

Even if your system is initially set up in a perfectly secure and pristine state, it will degrade over time. The more people with access to a system, the faster this degradation occurs. Therefore, the more administrators you have, the more often you should audit. Security scanning helps you audit the system to verify that your intended configuration is effective and up to date.

Benchmarking tools

Wouldn't it be great if you could see how other security experts have configured their Web servers, and then check to see whether your setup matches the industry best practice? The Center for Internet Security (CIS) (www.cisecurity.org) is defining consensus best-practice security configurations for computers connected to the Internet. Their free Benchmark and Scoring Tools provide a quick and easy way to evaluate a system and compare its level of security against minimum due care security benchmarks, which are kept up to date as new vulnerabilities are discovered.

Various reports guide you in how to harden both new and active systems while monitoring them to ensure that security settings continuously conform to the configuration specified in the benchmark. You can benefit from this knowledge, expertise and experience for free, so don’t waste the opportunity. By demonstrating compliance with an accepted security standard, you can help protect yourself from prosecution or regulatory sanction.

Monitoring services

Many organizations outsource the job of monitoring and testing their Web site’s security to a managed security service provider. The advantage of outsourcing these services is immediate access to experienced security specialists. This can solve problems of staff costs or shortages as it reduces the number of skill sets necessary in your security department personnel. The service level agreement will be an important part of the contract between you and your service provider, so look for firm commitments rather than vague assurances. The agreement should at least specify the following:

- ❑ 24/7 services
- ❑ Response times
- ❑ Customer reports
- ❑ Lapse times for policy changes
- ❑ Financial penalties for poor performance

Other useful tools, available for free, include those for mapping listening TCP/UDP ports to the program listening on those ports. TCPView and several other monitoring programs can be downloaded from www.sysinternals.com. A good file integrity checking tool is Osiris, available from http://www.hostintegrity.com. Microsoft offers pulist and pstat, which show detailed information about running processes, along with other Windows 2000 Resource Kit Tools.

Help is out there – Useful sites and services

It is imperative that you stay informed about security issues and take time each day to visit sites such as SearchSecurity, SANS, CERT and NTBugtraq, which provide bulletins, news stories and other related security information. You should also subscribe to their security bulletins or newsletters. Join the user groups and discussion forums run by the vendors of your hardware and software. Software vendors also provide a wealth of information on known security bugs for their programs along with possible solutions.

It can also be enlightening to visit hacker Web sites and monitor the postings and information available on them. These sites often provide tools that can be useful in your vulnerability testing. Google maintains a list with brief descriptions of such sites at http://directory.google.com/Top/Computers/Hacking/.