

► Network Security Tools and Their Limitations

Executive Insight Series by Brad C. Johnson

There are lots of tools that you can use to help analyze and profile the networked resources you have. There are web scanners like Nikto, WebScarab, and WebInspect; vulnerability scanners like Nessus and ISS and intrusion detection systems like snort. There are packet sniffers like Wireshark (formerly Ethereal) and TCPdump. There are specialty programs like the wireless tools Kismet, NetStumbler, and Aircrack or password cracking programs like Cain and Abel and John the Ripper.

There are several places you can learn about these tools such as <http://sectools.org>, <http://www.windowsecurity.com/software/Misc.-Network-Security-Tools>, <http://www.unixtools.com/security.html>, and <http://www.networksecurityjournal.com/features/open-source-security-tools-applications-resources-041007>, but of course you can use search engines to refine what you are looking for. If you haven't used network security tools before, starting with the programs listed in the sectools.org link is a good place to start.

You should use as many of these tools that are applicable to your environment as you can. Why? Any tool that makes it easier to administer and monitor your network is good. Any tool that helps you both manage your network and also keep it safer is even better. Of course, if you can use a free public domain or open source tool, instead of having to pay, that is even better still.¹ In any event, using tools is a good use of your time because they can help you identify unexpected changes in your environment and possibly identify specific exposures or vulnerabilities that may exist with minimal effort on your part.

Having said all these glowing things about tools, let's remember that most of them are only going to

find well-known "easy" to identify problems. In a very real sense, it is just like using virus detection software. Virus software is only going to find the problems it already knows about; it will not find new or slightly different variations unless it has been told exactly what to look for (which is why you have to update your virus definitions on such a regular basis).

These network security tools are not going to find subtle problems, they are not going to find combinatorial based vulnerabilities, and they are certainly not going to ferret out architectural or design issues that may plague your hosts, services, or web applications.

If you want to know if you have written secure code, you probably need to perform a code review. If you want to know if your web application ensures that unauthenticated users cannot access data reserved for authenticated users or that authenticated users cannot either view other's data or escalate privileges, you will need a hands-on assessment done by people who understand both high level design issues and low-level web application protocols. If you want to know if your host or network component like a firewall, router, or web server is properly configured, you are going to need a hands-on review to determine if it is properly hardened.

The bottom line is there is a time and place for everything. Using tools to perform routine scans and analysis on your networked services is something you should be doing on a regular basis. It is important, however, that you don't mistake this good "daily" hygiene with critically needed in-depth analysis that can only be performed at the hands of real experts.

1. Some organizations have policies that prevent the use of public domain software because they fear that the programs themselves will contain malicious payloads or cause unwanted side effects. If that is the case for you, for some programs, you can download and review the actual source code and generate the binaries yourself or there are some programs that have been vetted by independent organizations.