



Most businesses have a web site of some sort or other ... and just how critical is it to your business? For many businesses it has increased in importance in the last couple of years. The decisions you took when you set up the web site may no longer apply. Among those decisions were almost certainly the level of security or protection for your web site. In the light of recent events and the increased number of threats that organisations of all types and sizes face, those early decisions may now be out of date.

What are the problems that face you? Your web site could be hacked by someone (either inside or outside your company) and damaged. Your web site could face technical problems arising from outdated software or from the emergence of security holes in your software. You could face problems arising from the exploitation of security holes by worms, trojans or viruses. The overall consequence might not be terribly serious in terms of financial loss but it could be serious in terms of time, trouble and wasted resources. It could also result in financial loss to your organisation, though this is difficult to quantify – and even more difficult to get anyone to own up to having suffered it (most organisations prefer to sweep these sorts of disasters under the carpet).

None of this is particularly new ... and there are any number of tools out on the market which help you to identify your web site's problems. Many of the tools that are available have their limitations and the data they produce may be so huge that it is, effectively, useless. For many organisations facing the problem of how they determine the level of vulnerability of their web site(s), the best solution lies in bringing in an expert who can use the various tools and present them with a readable report.

ProCheckNet operates in much the same way as an expert (or a hacker for that matter) might. The developers claim a sort of artificial intelligence for the package in that it does not take a grunt approach to testing the security of a system ... it learns (or can be trained) to work on any system or platform. The service is not installed on your system but is run from ProCheckUp's servers – not least we conclude because this technology has the potential to break into any system and the security issues of letting this sort of technology into the public domain do not bear thinking about.

ProCheckNet



Supplier: ProCheckUp Ltd
Price: on application
Contact: +44 (0)20 7307 5001
 info@procheckup.com
 www.procheckup.com

FOR Great system for discovering security holes in your systems.
AGAINST New technology.
VERDICT This is a new approach to testing your systems to see if they have any vulnerabilities. Using AI (artificial intelligence) it works the way a cracker would and gives you an in-depth report on where your systems' weaknesses are.

Features	★★★★☆
Ease of use	★★★★☆
Performance	★★★★★
Documentation	n/a
Support	★★★★☆
Value for money	n/a
Overall Rating	★★★★☆

There are other benefits to running this system remotely – not least there is no overhead on your systems and no installation to have to worry about. Also you are always using the latest version of the software with the latest upgrades. The software is browser based – so you already have the means of using *ProCheckNet* installed on your system.

The use of an external system to attack your own web sites is well understood and organisations have used penetration testing for many years. *ProCheckNet* is located externally and using its artificial intelligence technology it mimics the hacking techniques that are used by crackers to break into your systems. However, unlike conventional basic scanners,

it operates in an intelligent way, altering its attack strategy based upon what it discovers when it hits your system.

This flexibility is reminiscent of the way that crackers have developed their attacks in order to defeat intrusion detection systems which might otherwise detect their presence and defeat them. This tool allows you to test your systems, which is particularly important in the light of the crucial importance of e-business systems – if this system uncovers a flaw that might have otherwise caused a security breach, it is well worth the fee.

The design of *ProCheckNet* differs from many of the existing tools – both public domain and commercial – in that it consists not of a single tool but instead a series of free-standing 'specialist' programs. Each specialises in communicating with a different protocol and is thus better able to focus on the minutiae of that particular protocol.

The specialist programs provide a channel for attack programs which exploit the communication efficiencies of the specialists. These attack programs use a database of vulnerabilities and check whether the vulnerability exists on your system. The database not only contains known vulnerabilities but also the circumstances in which those vulnerabilities can be exploited. *ProCheckNet* then goes one further and uses the discovered flaw or weakness to breach your system and discover further weaknesses.

The developers claim that the design of their product leads to more efficient and effective penetration testing. For example, complex protocols require a more sophisticated attack methodology – for example, crawling the system looking for weak points. The distributed design of the *ProCheckNet* system more readily permits this sort of testing and is more easily modified in the light of new vulnerabilities.

Keeping *ProCheckNet* up to date is relatively easy with this sort of design because it is so modular in construction. As new protocols emerge it is relatively simple to build a new specialist program. The attack programs can readily be modified in the light of new attacks emerging on the Internet and the vulnerabilities database can be constantly updated by reference to the various vulnerabilities as they are uncovered.

All in all, this new technology has the hallmark of a most effective way of uncovering your weak points and delivering a report which you can then use, bit by bit, to close the holes in your system. You can, of course, continue to use *ProCheckNet* to test whether your fixes have been effective.

[Ed note: The company says it has now improved most of its protocol 'attack' specialists, with application response identification. The system can also detect honeypots, and firewalls spoofing common services.]

Contact Information:

ProCheckUp Ltd



Syntax House
 44 Russell Square
 London
 WC1B 4JP

+44 (0)20 7307 5001
 FAX: +44 (0)20 7307 5044
 info@procheckup.com
 www.procheckup.com

