

Are you as secure as you think?

One company is changing the rules of security scanners by employing an entirely different approach: emulating how a real hacker infiltrates a network. David Ludlow assesses ProCheckUp's impressive new penetration testing service

Traditional security scanners are dumb in their approach. They respond to a user's request and blindly fire off all the selected attacks. As a result, running them is an art; you have to pick all the relevant attacks, but drop those that will either cause trouble or fail to work. And this is why security company ProCheckUp has changed the rules for scanners.

Its ProCheckNet hosted service works by emulating a real hacker. It performs a reconnaissance sweep of the targeted machine first. The idea is build a profile of the machine and only throw attacks at it that have a chance of succeeding.

The product is built around protocol specialists. Each specialist is designed to work with one protocol. They react just like client software, but syphon off the parts of the data that reveal information. This allows the specialists to see more as, for example, the HTTP specialist will deal with cookies, secure links, redirects and retries.

This is better than a standard scanner, which is often stopped by firewalls or takes down a machine because it isn't requesting data properly.

On top of this, ProcheckNet has the intelligence to work out the OS it is attacking and the applications running. At the front of this is banner matching. As administrators can often modify banners, other techniques must be used. One technique is to request a web page but change the case of the characters. Windows isn't case-sensitive, but Unix is. Together these make for detailed reconnaissance.

While the system is normally run as a service and the reports sent to customers, we were provided with a login to the system so that we could look at it first-hand. It's controlled through a web front-end with a range of settings that determine how the scan will work.

We were impressed with what we saw. ProCheckNet allows itself to be modified either to run in stealth mode or make a lot of noise. It can even act like a hacker and attempt to avoid security devices.

To get past an intrusion detection system (IDS) the system can use polymorphic code. This encodes URL strings differently to confuse the IDS pattern matching.

If you feel in a particularly self-destructive

mood, get ProCheckUp to turn on ProCheckNet's super stealth mode. This uses encryption to completely bypass IDS sensors. It might make you feel very insecure when first run, but the point of a security scan is to find out as much information as possible. Once the results come back, an IDS can be tweaked and reconfigured to start detecting genuine attacks.

For firewalls, the protocol specialists are used to check applications including FTP, SMTP, HTTP, POP3, NNTP and Imap. As the protocol specialists perfectly mimic a real

but ProCheckUp only runs those attacks that stand a chance of succeeding.

When it comes to attacking, ProCheckUp uses artificial intelligence to tailor attack signatures to the individual machine using the intelligence-gathering phase. Each attack signature is stored as a modifiable pattern to allow for this.

It's interesting to read the report at the end of an attack, as it shows how this works. We saw this when we attacked an IIS machine.

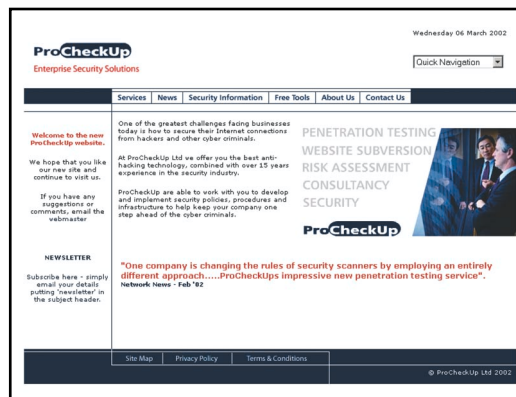
Most scanners will try and go for default files in directories such as scripts. If the administrator is sensible they'll change this default directory to another name. What ProCheckNet does is to scan the server and get a list of directories.

When it goes to the attack stage, it substitutes these names into the attack string instead of dumbly aiming for the defaults. This makes it much more likely to pick up things that other scanners will miss.

If the entire system seems like overkill for testing web sites, then ProCheckUp has an alternative product, ProCheckWeb, to help. This service is identical to its big brother, but only scans web servers and the services that they run.

Its sheer scope makes ProCheckNet very impressive indeed. It won't give you peace of mind the first time you run it, but you'll know exactly what needs to be changed. The IDS and firewall bypass features can prove that your systems aren't configured to stop a determined hacker.

However, as a hosted service it can only scan from outside your network. An agent that sits and scans internally would be better. After all, most attacks come from inside.



data exchange, firewalls believe traffic is OK, and let it through.

For more in-depth checks the scanner can be bumped up to test all ports and a wider range of applications. While these settings define the range that will be scanned, there's still the matter of what to do. This comes by defining the attack level. At the minimum, the scanner can stop at identifying systems. At the maximum it can perform a full-blown hack attack, including denial of service.

ProCheckNet can prove that systems have been breached by dumping a file either to a web server or a network file share.

Finally, the software can be set up to be really noisy and fill up logs, or to use stealth tactics and leave as little trace as possible. We ran scans on a few different machines to see if it really was as good as claimed. And, we have to say it was.

After selecting the kind of scan and attack level, we were ready to start scanning. We didn't have to worry about attack profiles or work out which attacks to run. The software did all of that for us.

The result is a faster and more accurate scan. In traditional systems, the scan time depends on the number of attacks selected,

PRODUCT DETAILS

Pros Fast; intelligently runs attacks; less likely to cause systems to crash

Cons Can't scan internally; must wait for a report to be generated

Price On application

Contact ProCheckUp

Syntax House

44 Russell Square

London WC1B 4JP

Tel: 020 7307 5001 Fax: 020 7307 5044

Web site www.procheckup.com