

The user's experience



It can be scary for an organization to undergo network penetration testing, as Ron Condon discovered from one company head.

For obvious reasons, most users are unwilling to speak on the record of their experiences of penetration testing, but the head of one company involved in online gambling was prepared to do so.

His first experience of using an outside company to do penetration testing should have filled him with confidence. "The company did a test for us last year and found no faults at all. As far as they were concerned, we had no security worries. To be honest, that was the worst kind of report I could have had," he says.

Unsatisfied, he followed it up this year with a second test, this time by ProCheckup (www.procheckup.com), a two-year-old privately-owned company that had been recommended to him.

ProCheckup runs a hosted service based in London (the company has just

incorporated in the U.S. and is planning a Boston office), where it will simulate hacker attacks on the client's systems. Rather than using the readily available open source tools favored by many companies, the ProChecknet service is built on ProCheckup's own technology, and incorporates a high level of artificial intelligence to mimic the cunning ways of a real hacker. For example, it can use polymorphic code to disguise URL strings and thereby pass unnoticed through an intrusion detection system.

Instead of bombarding the systems with attacks in the hope that one will get through, it does an initial sweep of the systems and focuses on inflicting the kinds of attacks that are most likely to succeed.

The approach certainly worked for our anonymous user. "They tore the sys-

tem to pieces. That was purely on sniffing. We operate 24x7 so the testers could not run any exploits or denial-of-service attacks. But they did find a lot of stuff, such as directories that were visible to the outside world with read and write permissions. They were eventually able to tell every operating system we were running, all the systems, what version of software, what fixes had been applied and what had not. It was quite scary."

Importantly, he did not have to wait until the end of the test to get the bad news. Each time a serious weakness was exposed, ProCheckup alerted him and provided a fix. These were then incorporated in the final report, alongside less serious flaws.

Had he been back to the previous company? "No, I saw no point in it. But they won't be getting any more of our business," he says. "There are a lot of companies offering penetration testing. It's easy for them to get a group of tools and to run them on your systems, and provide you with what comes out of the tool, without adding any value themselves."

His kind of business makes him as big a target as the banks, he says, so he has booked in for regular tests every six months.

"In an ideal world, we would have people in-house doing this kind of thing all the time," he says. "But in the real world, it just doesn't happen."

Ron Condon is editor-in-chief of SC Magazine.

Contact details:

ProCheckUp

ProCheckUp Limited
Syntax House, 44 Russell Square,
London, WC1B 4JP, UK

Tel: +44 (0) 20 7307 5001 • Fax: +44 (0) 20 7307 5044

Web: www.procheckup.com • Email: info@procheckup.com