Classroom breaches of top enterprises spur industry debate

Are student pen testers a threat to security professionals?

Darren Pauli (Computerworld) | 18 October, 2007 11:03 | Comments | Like

Page: 1 2 3 next >

Penetration tests conducted by a group of non-IT students has set the cat among the pigeons in the security community, spurring analysts and security professionals to emphasise the importance of certified penetration tests.

The results of the tests, announced last week, found severe network security flaws in 79 percent of the 200 largest Australian enterprises surveyed.

The tests, held at the Australian Graduate School of Policing, saw 25 non-IT students breach security infrastructure and gain root or administration level access within the networks of Australia's largest companies, using hacking tools freely available on the Internet.

Computerworld readers questioned the motives behind the test, the methods and tools employed and the level of legal clearance required to conduct the examinations.

LogicaCMG chief security officer Ajoy Ghosh, who headed-up the test, said it is performed about twice a year, and was conducted to show the students made up of lawyers, prosecutors and criminal investigators how hackers can steal confidential data.

"It was an opportunity for them to experience for themselves the opportunities that hackers have online," Ghosh said.

Computerworld reader and Asia Pacific general manager at security-assessment.com Drazen Drazic was one of the respondents who expressed concern that the tests could devalue professional penetration testing in the eyes of business managers.

"Anyone can get free hacking tools off the Internet and hack to a certain level, but it takes many years of experience to be able to do a penetration test to a level where you can give a CEO a good snapshot of their security vulnerabilities," Drazic said.

"It would surprise me, given Ajoy's industry experience, that the message was that anyone can do penetration testing because some CEO's could read it and think they can get one of their [non-security professionals] to do it instead of paying $20,000 for penetration tests."

Debunking penetration tests was far from the objective of the project, according to Ghosh.

"A number of my peers have raised the issue (voiced by Drazic) saying 'how dare you go out and show how easy penetration testing is' - but it is what it is - it was not a professional penetration test, it was a classroom exercise conducted by non-IT people," he said.

"I would expect a professional penetration test to include a lot more technical testing and to undercover a whole suite of problems over and above what we did."

Another respondent, Big Galoot, posting on Drazic's IT security blog Beast or Buddha joined others in expressing concerns about the legality of the tests.

"Either you accept as fact that the top 200 companies knowingly allowed their systems to be hacked by a bunch of uni students, or you don't. As a shareholder in some of the top 200 Australian companies, I'm very annoyed and I will want answers as to why they allowed the exercise to proceed," the blogger wrote.

Internet services company Biko Technolgies director of technology Greg Kowalski was equally concerned about the tests. He asked of the legal status of the intrusion attempts, and whether they are considered separate to unauthorized criminal hacks.

Legal clearance was not required for the tests, according to Ghosh. Web site owners, including CEOs and C-level managers, were contacted to obtain permission to conduct the tests, and were asked not to inform IT staff to allow "responsiveness" to be assessed.

A range of free hacking tools were used, however each test first established a network fingerprint using N-Map, ran vulnerability tests with Nessus and used Nikto to map "Web application vulnerabilities".

Students were handed a CD containing the tools to save time sourcing the applications, however Ghosh said they can be downloaded from some 30,000 Web sites.

He said some of the vulnerabilities were exposed by discovering access identities through social networking techniques, where students tracked connections between employees to discover passwords.

The class adapted easily to the social networking methodology because, having all completed the National Strategic Intelligence Course, many had already applied the technique to drug or terrorist investigations.

Students were given a one day crash course on how to use the applications and networking techniques to extract information, however it was unclear whether those methods were used out of necessity or to fulfill class requirements.

Christian Heinrich, an organizer for the Australia and New Zealand Snort User Group, attacked Ghosh's claims that freeware IDS, such as Snort, "does not have to be expensive", and said the program's operation costs add up, including release cycles and updating and writing specific implementation rules.

"In addition to the hardware costs, which exponentially increase depending on bandwidth, the initial build of Snort requires a significant level of technical knowledge [for] Snort and its dependent packages, such as libpcap, MySQL, Barnyard and Sguil," Heinrich said.

He said the cost "exponentially increases with the need to repeat the same procedure for each host dedicated to Snort".

The Web application layer poses the biggest challenge to penetration testers, according to Drazic. Testing at this layer, which is where most of the biggest attacks occur, requires in-depth knowledge of coding including application code and development.

Many commercially available application vulnerability scans won't cut it either. The applications, according to internal tests conducted by security-assessment.com, could only detect 13 from 35 vulnerabilities in a set environment.

Vulnerability assessment, widely regarded as akin to penetration tests, demand a similar level of experience.

Vulnerability assessment tools, such as Qualysguard (which security-assessment.com sells) highlight a range of server and operating system vulnerabilities, but Drazic said only a professional can understand the relevance of the results and use them to see what can be comprised.

Gray hat hackers, offering dirt cheap penetration tests for as little as $500, have helped taint the image of professional penetration testers.

In an article which appeared in Computerworld's sister magazine, Chief Security Officer (page 38, July, 2006), Gartner security analyst John Pescatore said hackers, often students, have driven some professional testers out of the business by undercutting prices by more than 80 percent.

However he warns that cheap tests are risky for business because they do not construct exercises that reflect the complexities of a corporate network.

Mark Weatherford, CISO for the state of Colorado said in the same article that business must tighten network security and plug vulnerabilities to get the most out of a penetration test, and to avoid damaging poorly built systems.

"People think that you can push the easy button and it will happen, your problems are clear. It just points out that your system can be exploited. Big deal," Weatherford said.

"I consider a pen test to be the supreme test for a mature organization. It's important to remember that pen tests are invasive and can break things."

Have an opinion on this story? Click to e-mail Darren Pauli.

RELATED WHITEPAPERS

- For PCI, the Future is Now
- Hassle-free compliance | A CSO guide to operational security
- Bandwidth Bandits
- Legacy Tools: Not Built for Today's Helpdesk
- Beyond PCI Checklists: Securing Cardholder Data with enhanced File Integrity Monitoring

COMMUNITY COMMENTS

- "Thanks very much for the link. It is another example of you ..." on Opinion: We need to think in multiples on broadband
- "There is already proof that CP sites can be removed easily. Someone ..." on Child porn filter coming mid-2011
- "So now it's 450 CP sites that ACMA havn't done anything about. ..." on Child porn filter coming mid-2011
- "@55, umm no... wrong again (at least you are consistent)... Mine is ..." on Opinion: We need to think in multiples on broadband
- "I can't believe Conroy keeps accusing everyone of being interested in child ..." on Filter cops criticism in cyber-safety commitee