

Home /



Sign up for the *MIS* newsletter!

Ethical hackers doubt ethical hacking

Tuesday, 07 August 2007 | Michael Crawford

IT Security experts and enterprise firms alike refuse to acknowledge the term "ethical hacking", with many seasoned and expert practitioners simply refusing to use the term to describe their position or skill set.

Even training companies who offer "ethical hacking" courses distance themselves from the stigma of associating themselves with hackers. Generally the courses are geared towards effective penetration testing for staffers in an IT shop and taught by penetration testing firms due to the nature of the work.

Rob McAdam, owner and director of penetration testing and corporate security training firm Pure Hacking, said running a business solely teaching enterprise IT staffers the ins and outs of penetration testing is fictitious. McAdam said in comparison to IT security consulting the interest is very small.

"All the people we train in here have all got a basic interest in security and have a personal value associated with security but the interest from enterprise in training someone, in comparison to using a security consultancy to perform a penetration test, is very small," McAdam said.

"All the major Australian banks have their own internal penetration testing teams as in order for cost effectiveness they have to have these skills on board but still in many cases internal policy dictates an external consultant must also conduct an independent penetration test of the organisation.

"IT managers are the core of our students but we also see some network administrators but never any CIO as their decisions are much more strategy focused and the penetration testing courses are practical."

McAdam frowns upon using online tools to ease some of the more painstaking tasks of training people on network security. Ernst and Young rely on teaching people on using "leading edge exploit tools" as part of their eXtreme Hacking Workshop.

Bruce Young, Ernst and Young partner of technology and security risk services said many times the staffers attending the course are sponsored by the CIO and are usually the ones charged with configuring systems or an IT manager attempting to better understand the security risks their organisation faces.

Young said attendees from large organisations at the workshops are typically of a junior IT practitioner level whose job it is to better defend the organisation.

"Some organisations don't even feel comfortable attending such a course if it is shared by other people from different organisations so we have to hold dedicated courses and that allows people to talk amongst themselves," Young said.

"The interest is now beyond 'ethical hacking' and now to help organisations prepare themselves for building web applications, another area organisations have put a lot of investment into so instead of teaching more traditional 'hacking' skills we are helping web developers code better applications.

"We were focused on ethical hacking into infrastructure of the organisation and then as organisations configure infrastructure better the perpetrators look for easier points of entry and focus on the application itself... this is part of the natural evolution in the way attackers think and organisations respond."

Young added teaching such courses is a double-edged sword.

"On one hand, people argue that we are teaching people how to be hackers but we certainly screen people in course, then the majority of attendees are sponsored by an organisation to protect their organisation," Young said.

Drazen Drazic, general manager of penetration testing and IT security firm Security-Assessment.com, said those in the industry coined penetration tester can also claim to be ethical hackers, however Drazic said he hates the term.

Drazic said some companies do trade on the hacking name but at the end of the day it is all the same stuff.

"They all should be called security researchers, never ethical hackers as it is just a superfluous term."

Email Story

Print Story

Bookmark Page

Add to Facebook

Add to del.icio.us

Add to Diigo

Add to Reddit

Add to Slashdot

Add to StumbleUpon



Be the first to comment on this article

MISAustralia welcomes and encourages reader comments. Please note that any comments posted will be subject to the MISAustralia [Publication Guidelines](#).

Post your comment

Note: Fields marked * are required.

Name:*

Email:*

(will not be published)

Comments:*

Submit

The first thing we want to do is align a print and document solution with your business objectives.

▶ [CLICK HERE TO FIND OUT MORE](#)



Canon
advanced simplicity

sponsored links



UC&C Evolving Business Communication

IDC Vendor Spotlight discusses the latest trends in UC&C

Making property investment easy

Invest in secure, worry-free property With Defence Housing Australia.

Get the first mover advantage!

Dealbook, stay a step ahead.

FREE 14 DAY TRIAL – click here.



multimedia



The Future of Media

Mon 16 Nov 2009 5:49PM

Social media has disrupted marketing and journalism. So what happens when everyone including companies and government agencies are making content? The Scoop's "Future of?" series kicks off this week with Andy Gregson, founder of Media140 and Annabel Crabb, political columnist at the Sydney Morning Herald.