"How UNSW creates the world's best hackers"

by Ben Grubb via lyx - SMH *Monday, May 13 2013, 1:13am*
international / prose / post

> So ran the headline in the IT section of the SMH; to put it simply a 'slight' exaggeration or more accurately, a well over the top claim, Mr Grubb -- is someone from UNSW giving you head?

Indeed, the headline elicited immediate bursts of laughter from the REAL hacker underground; the student participants in the Challenge know full well their level of expertise regardless of the over-the-top, headline. A few facts should be noted before jumping to any hasty conclusions and to gain a proper perspective on the situation.

The test scenario was set up by the ADF or Oz Defence Forces -- LOL -- and never was there a greater bunch of IT lamers in Oz except for the AFP (Feds) who won't move on an IT crime unless there's a headline in it for them. Yes, we have 'experience' -- digital and social -- with both lame government departments and it is enough we mention only the above. We are Aussies too and do not wish take credit away from the young, hopefully not too naive, students for their efforts, though we suspect they are aware the 'Challenge' was literally child's play -- are you reading this Mr Grubb, a little perspective in future, please?

We also note a reference to failed Aussie hacker Assange in the comments section, what a thorough disappointment he IS -- he broke the cardinal ANONYMITY rule and is now paying the price, doh! And everyone claims he is 'gifted!' Perhaps an article about him, Mr Grubb; he could have easily released all that info without breaking cover -- you simply post it! Let's hope the new generation of hackers does better than Assange. Indeed, we all have faults and that is the point, isn't it Julian and Mr Grubb?

SMH story follows:

> The University of NSW is known for producing some of Australia's top lawyers, doctors and accountants. But the 64-year-old institution is now gaining a reputation for excelling in what is often viewed as anti-establishment – hacking.
>
> It's noon on Tuesday and a group of four students are hovering over their laptops having just bunkered down in a room at UNSW's Kensington campus, where they're going to be for the next 24 hours hacking into IT systems. Computer cables, power boards, water bottles and brown paper bags full of food are spread across the table.
>
> Looking over the students' shoulders is their admired IT security lecturer and mentor, who likes to distance himself from being called an academic, laughs off the suggestion he's a "hackademic" and doesn't want his photo taken for this article for undisclosed reasons.
>
> By noon on Wednesday the students have barely had any sleep. This is because they have just finished participating in the 2013 Cyber Security Challenge, which Telstra, along with government agencies, held last week. It's the second year the challenge has

been held and Telstra says it holds it to help identify potential candidates for IT security work, which are in demand.

The challenge involves students, from universities and TAFE colleges nationwide, competing in a non-stop 24-hour "capture the flag" contest, where they test the security of a fictitious company's IT systems, aiming to get the most points.

During the 24 hours they are required to conduct "penetration testing" on the company's web apps, network and product, as well as give advice in easy-to-understand "grandma" language.

A penetration test is used to evaluate the security of a computer system or network by simulating a hacker attack.

Forty-three groups, each made up of four students from 20 institutions, participated and it proved so popular that Telstra had to cap the number of teams per school to three. What may have attracted the budding young hackers was the first prize, a trip to the infamous Black Hat IT security conference in Las Vegas.

UNSW entered three groups of four students in the challenge, placing first, second and third. The winning group also won last year.

Some members of the winning team have also come first in other Australian security challenges, such as the Ruxcon capture the flag contest held in Melbourne.

So what is it about UNSW that is cultivating some of the nation's most promising young "white hat" hackers?

Fionnbharr Davies is the IT security lecturer and mentor to the UNSW students.

Unlike other, more serious academics who teach at the university, Davies lists as a joke on his staff profile that he is a "Professional Suit Wearer" who teaches "Haqr techniques", "HTML" and "Thwarting the lizard people threat".

A 27-year-old who works full-time at Azimuth Security, Davies co-lectures part-time alongside Brendan Hopper, 28, who works at the Commonwealth Bank as a penetration tester.

Many of their students have gone on to work at large security companies such as Stratsec (now BAE Systems) and Securus Global, while some pupils are doing internships at the likes of Google.

Theo Julienne, one of Davies' students and a member of the Cyber Security Challenge winning team, said that what made him a good white hat hacker was Davies' unconventional teaching practices. Julienne's teammate Karla Burnett agreed. Both students said Davies' courses were practical and hands-on, rather than all about theory.

"If companies are doing stupid things that do not make sense he criticises them in lectures," Burnett said. "He won't try and be polite about stuff."

Julienne added: "[Davies] doesn't screw around with theory stuff. He tells us this is how

it works and this is what you do in a company to secure it."

Although working in the security industry pays more than lecturing, Davies said he lectures because it is fun.

"I've actually not been paid twice because I was too lazy to fill out the forms because I'm not motivated by money," he said.

"It's incredibly rewarding to teach students and see them do really well... My students winning first, second and third place [last week] is great."

He said his courses are very different from the typical IT courses at other universities.

"It's a really big difference from your [average computer] science degree courses, because generally when you are going to them you start doing artificial intelligence [AI].

"You get told here's a problem, here's the algorithm you should use to solve it, and go and solve it using that algorithm.

"So essentially this [security] part of the course I teach is like a mini thesis. We drop the students in the deep end and go, 'All right, you have to come up with your own project. It's going to be difficult and we'll judge you half on it.'

"A lot of people then immediately drop out of the course after the first or second week when they realise it's going to be a ton of work. A lot of university students don't want to do a ton of work."

Davies said he was shocked when he saw the way students at other universities were taught IT security.

"They're all taught by these academics who have never hacked a thing in their life," he said. "The students are good, it's just the teachers ...

"Talking to some of the other students at other universities I was actually quite appalled at the sort of things they were taught. Like, it's not even real computer science."

Davies said about 60 per cent of his course focused on projects, while the other 40 per cent was based on a "war game" challenge like the one held by Telstra and government agencies.

"So students write rootkits," he said. "At the courses running at the moment ... students are designing rootkits for Mac OS X, Android and Linux."

A "rootkit" is a stealthy type of software designed to hide the existence of certain processes or programs from normal methods of detection. It is often malicious and used by hackers.

"People are writing exploits in the course and doing large security projects you might normally see proper security researchers doing [in the real world]," Davies said. "But students can do them because they're intelligent and motivated."

To defend against hackers, Burnett said, one needed to think like one, and that was what Davies taught students to do – by thinking "offensive" rather than "defensive".

"You need to know how a hacker is thinking if you want to defend against them," Burnett said.

Davies, when asked if he believed students should report vulnerabilities they find or stumble across on company's IT systems, said: "We say that you should do whatever you want with the exploit. It's your vulnerability, you found it, it's your thing. You have no obligation to report it at all. In fact, reporting it can get you into a lot of trouble."

Davies pointed to the case of Australian security expert Patrick Webster, who received a knock on the door from police and a legal letter after he told First State Super he had found a flaw exposing the personal details of its 770,000 members.

First State Super disabled his superannuation account with them, asked to check his computers and said he may have been liable for any costs to fix the security breach he reported to them.

"There is always the chance that a company will turn around and bite you," Davies said.

"That kind of shit happens all the time and is why I actually recommend not doing responsible disclosure. I don't like the term and if anything you should sell the vulnerability.

"Sell it to anyone [you can find] because they're the ones who will then deal with the company... Or, if you're not going to reveal it, go through a third party like CERT Australia."

Matt Barrie, who teaches cryptography and network security at the University of Sydney, said his course was also very hands-on, and to an extent unconventional, but not as much as Davies'.

"We get people to analyse things like Wi-Fi, find out how it can be hacked and what the problems are," he said.

Barrie also conducts war games and gives students cryptographic puzzles to crack.

But unlike Davies, Barrie believes universities are "getting fairly practical" with their IT security courses.

"Some of my graduates have joined the Defence Signals Directorate and have become key people at a firm called Stratsec, which recently got sold to [Defence contractor] BAE Systems," Barrie said.

Asked if he thought he could be creating the next generation of black hat hackers, Davies said: "I have absolutely no fears I'm creating some black hat army. If anything, these students are going to go on to become really good [white hat] security researchers.

"I think if people were going to be black hats they'd be black hats by the time they hit

university."

[I'll let you in on little 'secret', Mr Grubb; elite hackers do NOT work for governments or corporates -- they have no need, doh!]

http://tinyurl.com/c6jar5g
