;login:

THE MAGAZINE OF USENIX & SAGE

April 2002 • Volume 27 • Number 2

inside:

POINT/COUNTERPOINT

BY TINA DARMOHRAY AND ROB KOLSTAD

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

point/counterpoint

At Who's Expense?

by Tina Darmohray

Tina Darmohray, co-editor of *;login:*, is a computer security and networking consultant. She was a founding member of SAGE.

tmd@usenix.org

The local DA has expressed an interest in talking to me about a break in to Lawrence Livermore National Laboratory's computer systems. Apparently she is looking to gain insight about typical Laboratory computer security and incident response from folks who have worked at LLNL. As her contact went into more detail, I realized that I knew both the "hacker" and the "hackee."

The break in incident in question was reported in September of 2000:

"A 21-year-old Minnesota computer employee was arrested at home on Monday for allegedly hacking into the Lawrence Livermore National Laboratory. Benjamin Troy Breuninger, known on the Internet as "konceptor," had not jeopardized the lab's classified nuclear research material, but he allegedly accessed the lab's administrative information, causing about $50,000 in damage. It appears that the attack was random and that Breuninger didn't have any personal gripe with the lab."

Once they mentioned the names "Ben" and "Konceptor," I immediately remembered that I had met Ben in October 1998 at a conference in Orlando, FL. I taught a tutorial with Phil Cox at that conference. In the evening session following our tutorial Phil was the "White Hat" and Ben was the "Black Hat" in a "Hackers and Defenders" session that had been arranged by the conference.

We didn't know Ben prior to the session, but when we saw him it was immediately obvious that he was "just a kid." Despite that, he held his own technically. The depth of his knowledge was impressive. He clearly had a handle on the fundamental workings of the Internet. He was well versed in such areas as DNS, ports and services, and a wide array of protocols and programming languages. He described in detail how he and his peer group spent their weekend nights: his phone buddies would hijack a phone line off an office building and they'd run a long wire into the bushes where Ben would sit w/his laptop and do the "cracking." Many folks from the audience told Ben they didn't like what he and "his kind" were up to. Ben's stance was that they were just having fun, learning, and, bottom line, not hurting anyone.

After the presentation Phil and I cornered Ben. We learned that he was indeed just a kid: old enough to drive, but I don't think yet old enough to vote. He said he'd never been out of his home state, and that this was his first trip on an airplane. It was obvious that while Ben was well versed in the Internet, he wasn't worldly in any other way. During our conversation, Phil and I tried our best to persuade Ben to apply his knowledge in legal ways: college, career in system administration.

Looking back, I have to wonder about the message Konceptor's all-expense-paid trip to Orlando sent to him and whether it amounted to unintentional exploitation. It's easy to understand why Konceptor didn't take our advice. Why should he? His hacking hobby had just landed him his first trip on an airplane to a conference where a room full of adults listened to what he had to say. At his age, that had to be huge for him, as well as among his friends. From his perspective, his hacking had paid off big time and he was being taken seriously. Hindsight suggests Ben's perception, as well as "his own good" should have been more carefully considered.

Counterpoint

by Rob Kolstad

Ben is surely walking the wrong path, especially for a 21 year old who absolutely should know better, having been told so repeatedly. Of course, he is not the only one. His life is now going to be dramatically more complex and challenging as he deals with both the legal system and lawyers while learning that our country really does have absolute rules that, when broken, can have severe penalties.

The main questions are: was his trip to the security conference exploitative? Was it a reward for "being bad"?

Tina mentioned the black hat/white hat presentation at which the participants were squarely put into roles ("good" vs "bad" – or maybe even "good" vs "evil"). Just as Ben had not been out of his state, similarly most participants had not seen a "hacker on the hoof." Tina mentions his apparent lack of worldliness and it was extremely apparent in any dealings with Ben.

I think it can be argued that the opportunity to come to the conference to share – and to meet the security community – had a huge potential for good. This clearly naive kid had the opportunity to see, meet, and greet professional security people and learn all about the potential for employment and gratification in that part of our economy. I can imagine no better way to stimulate someone to move into a more productive role than "system cracker for fun." I know I spoke to him one-on-one as did a myriad of other attendees. I imagine (without direct knowledge) that the messages he was sent were clear and consistent.

As happens often, Ben made up his own mind, unswayed by the 2,000-fold members of the "opposition". He will learn first-hand that "just having fun" is perceived by others in a different way. Some people will never be able to participate in our society in a reasonable way; more's the pity.