

## It Wasn't Me

Investigating computer crime or misuse is always challenging in a large networked environment. Knowing which account was used is a clue, but usually not more than that. The real question for us as forensic investigators is, "Who used the account to commit the crime?" I have learned by experience that more times than not, when the owner of the account is confronted with the evidence I can expect the response, "Yup, that's my account alright, but it wasn't me". The reality is that sometimes your suspect is telling the truth and sometimes they are not. Which leaves us with the question "Who committed the crime?"

Obtaining user accounts and passwords in a given organization is relatively easy. The user account is usually made up of a combination of the first and last name of the user. Certainly if you work at this organization you will know that for example, last name and first initial is how the organization structures user accounts. So, that leaves the password which is easy to get. The organizers of the Infosecurity Europe 2004 conference found that 71 percent of office workers were willing to part with their password for a chocolate bar. 37 percent of workers immediately gave up their password and an additional 34 percent gave up their password with a little coaxing. My favourite is to call someone in an organization who doesn't know me and pretend to be someone calling from the help desk. (As an aside, if you want to appear as being an inside caller, simply call someone in the organization and have them transfer your call to the extension that you wanted to go to in the first place.) After a little story about how you can see that there is a virus on their computer and you immediately need their user account and password to sign on to their system to eradicate the virus which is threatening the corporate network, few will stand in the way of giving you their password. So, as investigators we need to be aware of the fact that the suspect may or may not be telling the truth when they say, "That was my account, but it wasn't me".

Every case is different, but here are a few suggestions on how to proceed. After doing the preliminary investigation you need to make a decision on whether you feel the person who owns the account is responsible for the action. If you feel they are not, then they could become a valuable source of information. Questions like, "Who had access to your password", "Have you written down your password", "Have you ever given your password to anyone, like the help desk" or my personal favourite, "Don't tell me your password but tell me about it, things like is it a dictionary word, is it easy to guess, is it a pet or family member, does it have characters or numbers in it". This will give you some insight into who may be behind the crime. If one of the answers is, "It is my mothers maiden name", then the next logical question, assuming they didn't give their password to anyone would be, "Who knows your mothers maiden name?". I had one individual tell me that they had used the same password for the last three years, however, they remember writing it down recently in the back of their pocket notebook which has gone missing. That is likely how the password was compromised they said. For you clever investigators out there I am sure you can see the contradictions in that statement. If you

had the same password for the last three years you certainly wouldn't need to write it down to remember it. This helped focus the investigation on the right suspect.

If you feel that the person responsible for the crime is the same person who owns the user account then talking to them at this point in the investigation is a bad idea as it will obviously tip them off to the investigation. Several things should be considered. First, can you tie the individual to that specific computer at the time of the crime (I use crime in a broad sense to include any misuse of corporate assets). Can anyone verify that they were at or near the computer at the time of the incident. Is there any video (public lobby) that can show the individual in the building at the time. We need to look carefully at the activity of the account in question at the time of the incident to give us the greatest insight into who is behind the crime. Let me give an example. If I wanted to send a nasty note to my boss and do it under the guise of another user account it would seem reasonable that I would minimize the amount of time that I was signed onto that account. In other words, I would sign on, send the message and sign off. Which leads us to ask more questions. Who was signed on to that computer just before the incident. Who was signed on to that computer just after the incident. Did either of those people see anyone use that computer at the time in question. Be careful of course, because one of those people may be your suspect.

Another example may help. Let us say that someone downloaded a "hacking tool" onto a particular computer and was launching attacks against certain servers that contained critical financial information to your business. Unfortunately, you don't find out about it from the network people until 3 days after the fact. You do know that the attacks were unsuccessful, however your job is to find out who is behind it. We know which computer launched the attack and a simple check will enable us to find out who the file owner is. We also determine that the account used, signed onto the computer 1 hour before the file was downloaded and then immediately launched the attack against the server. The attack ran for 2 hours and then the user signed off. We check to see if there was any email activity at the time that may give any clues. However, we find there was none. Another extremely valuable piece of information is to pull the internet usage logs. I personally prefer to go to the native Microsoft proxy logs as I find it gives the best and most detailed information. Canned reports, like those found in Websense give good summary reports but lack the level of detail I am looking for. The internet usage prior to the event of downloading the "hacking tool" is key. In this case the person using the account used [www.ask.com](http://www.ask.com) for their internet searching which is not as popular as yahoo or google. The person also visited the site [www.bankofamerica.com](http://www.bankofamerica.com) as well as a [www.fishing.com](http://www.fishing.com). These pieces of information can now be used in profiling our suspect. By looking at the proxy logs for a period of time (say the past 6 months) we will find that that not too many people visit all three of these sites. People tend to be creatures of habit and go to the same sites usually around the same time of day. We have our favourite search engine, our favourite online newspaper and our favourite stock site.

You could argue that you didn't download the hacking tool and that someone stole your account information. It would be difficult to argue the fact that you, and you alone are the only person in your organization that ever went to 3 particular sites over the last 6 months

and that the person who stole your account information also follows the same profile as you. “It wasn’t me, it was my cloned twin brother!”