SECURITY - THE FINE LINE

Information security. Hackers, war-driving, rainbow tables, sql injection, buffer overflows, and many more terms lend this field an aura of mystique and exoticism. It all sounds so cool, no wonder people want to get involved, both on the side of the angels and on the side of the devils. You get this idea of some battle between good and evil. But is it so? Not always, believe it or not. There are many instances that are not always clear cut for everyone, this is where a security practitioner's code of ethics comes into play, along with a large dose of understanding the issues. Lets take a look at some things..

Security Tools

There are many tools around, passwords crackers to port scanners, and all the ones in-between. And we have all heard the stories about how the bad people use these tools and how bad they are, but are they really? So see, a password cracker tool can be used by an attacker to find passwords to help attack systems, while an administrator can use the same tool to perform the same task to try to prevent this very attack. The point here is that the tools themselves are not bad, rather the intentions behind there usage can be.

Ethical Hacking

Is there such a thing? I think so. Many of us have had to do investigations for a company against a staff member, and in the course of these investigations we may use the exact same tools and methodology of an attacker. We may even be looking for the same thing that the attacker is, the difference is one small thing - we have the permission of the company owners. And that is that. Or is it? Many people feel that due to pervasive aspects of technology, such investigations are actually an invasion of the staff member's privacy. Or even if the corporate policy is airtight enough to dismiss such concerns, where does the investigation stop? Say you are investigating a certain issue, and while doing so you come across something else, what do you do? Let's take that a step further, lets say in the normal course of investigating a desktop or network fault, you come across material which is against corporate policy (I state this specifically because if the material is something which is unlawful, then you have no choice but to report it)?

User Friendly Security

First off, I do not think there is such a thing. Security is the enemy of ease of use, users would love a system where everyone just access whatever they need without having to worry about pesky passwords or overly-restrictive access rights. To some users this is the ultimate computer system. But to all the other people out there either having heart attacks, or wondering what this company's IP address range is, such a system is an open target. You see each bit of security generally costs some ease of use, very often each feature is a new attack vector. For example, passwords - when a good password policy is put in place it forces users to choose good passwords and periodically change them, but for users such a system is just a headache. Now I know I have used examples which are blatantly obvious, but what about those that are not so obvious? What if you disallow people to access Google? Do you have a good enough reason to do this, what security benefit do you get which is worth the cost in ease of use? This whole question can be very tricky, because very often we may be the only people who can understand the trade-off.

Disclosure

When a security researcher finds a new vulnerability what should they do? When they tell the vendor, how long do the wait for the fix before going public to place pressure? Should they go public? Should a public announcement be made how much detail should be given? Should the actual exploit code be published? This whole question is still a hot topic, and will continue to be one until we have perfect systems. You see security through obscurity does not work, but it is not responsible to not allow the vendor time to fix the hole. There is also the view that the public should know, not only to better secure themselves but also so that they know what products to use and which not to. Personally I think that keeping all of these things in mind, but in balance is something that can generally only be done on a case by case basis, but at the end of the day the public needs to know where the problems are and how to protect themselves.

Tinkering

Should we tinker? Is it right to bang away on software to see when and how it breaks? Is it right to even look for vulnerabilities? This is one of those things I think we will never get away from as long as there or those who would use these flaws illegally. You see for as long as there are those who will try to victimize us, there will need to be people to protect us, and those people will need to know how the bad people operate. Bit of a strange circle is it not? We need to find the holes in order to protect ourselves, in this world, what you do not know can hurt you, and if it is unexpected it can hurt you badly.

Final Words

These are just some of the fine lines of information security, some of the issues which security practitioners need to navigate their way through as they fulfill their duties. There are many others but these are probably some of the more common ones. There are no clear cut answers, but the one thing to always keep in mind is to do no harm, always make sure you can look yourself in mirror. Let me repeat something I have mentioned previously..

> "Let those who hunt monsters, be careful that they themselves
>
> do not become monsters. For when you stare into the abyss,
>
> the abyss stares back."
>
> -Fredrick Nietzsche-